Nmap Scan Report - Scanned at Fri Sep 27 14:40:19 2024

Scan Summary

Nmap 7.94SVN was initiated at Fri Sep 27 14:40:19 2024 with these arguments:
/usr/lib/nmap/nmap -A -p- --script all -oA report-2024-09-27_14-40-19-192.168.50.100 -T4 192.168.50.100

Verbosity: 0; Debug level 0

Nmap done at Fri Sep 27 15:59:14 2024; 1 IP address (1 host up) scanned in 4735.37 seconds

Pre-Scan Script Output

Script Name — **Output**

broadcast-listener

```
  ether
      ARP Request
        sender ip    sender mac         target ip
        192.168.1.1  08:00:27:35:4e:1a  192.168.1.105
  udp
      DHCP
        srv ip       cli ip         mask           gw           dns          vendor
        192.168.1.1  192.168.1.103  255.255.255.0  192.168.1.1  192.168.1.1  -
        192.168.1.1  192.168.1.105  255.255.255.0  192.168.1.1  192.168.1.1  -
```

hostmap-robtex

```
*TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
```

http-robtex-shared-ns

```
*TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
```

targets-ipv6-multicast-echo

```
  IP: fe80::a00:27ff:fe35:4e1a  MAC: 08:00:27:35:4e:1a  IFACE: eth0
  Use --script-args=newtargets to add the results as targets
```

broadcast-dhcp-discover

```
  Response 1 of 1:
    Interface: eth0
    IP Offered: 192.168.1.105
    Server Identifier: 192.168.1.1
    Subnet Mask: 255.255.255.0
    Router: 192.168.1.1
    Domain Name Server: 192.168.1.1
    Domain Name: home.arpa
```

targets-asn

```
  targets-asn.asn is a mandatory parameter
```

eap-info

```
please specify an interface with -e
```

192.168.50.100(online)

Address

- 192.168.50.100 (ipv4)

Ports

The 65438 ports scanned but not shown below are in state: **closed**

- 65438 ports replied with: **reset**

The 67 ports scanned but not shown below are in state: **filtered**

- 67 ports replied with: **no-response**

Port		State	Service	Reas
21	tcp	open	ftp	syn-a

ftp-anon

```
Anonymous FTP login allowed (FTP code 230)
```

ftp-brute

```
  Accounts: No valid accounts found
  Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
  ERROR: The service seems to have failed or is heavily firewalled...
```

ftp-syst

```
  STAT:
FTP server status:
     Connected to 192.168.1.101
     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-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://www.securityfocus.com/bid/48539
      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
```

banner

```
220 (vsFTPd 2.3.4)
```

22	tcp	open	ssh	syn-ac

ssh-brute

```
Accounts: No valid accounts found
Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
ERROR: The service seems to have failed or is heavily firewalled...
```

ssh-publickey-acceptance

```
Accepted Public Keys: No public keys accepted
```

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)
```

vulners

```
cpe:/a:openbsd:openssh:4.7p1:
      95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A
      2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A
      CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
      CVE-2016-1908   9.8     https://vulners.com/cve/CVE-2016-1908
      B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23
      8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623
      8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC
      5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A    9.8     https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A
      CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
      SSV:78173       7.8     https://vulners.com/seebug/SSV:78173    *EXPLOIT*
      SSV:69983       7.8     https://vulners.com/seebug/SSV:69983    *EXPLOIT*
      PACKETSTORM:98796       7.8     https://vulners.com/packetstorm/PACKETSTORM:98796       *EXPLOIT*
      PACKETSTORM:94556       7.8     https://vulners.com/packetstorm/PACKETSTORM:94556       *EXPLOIT*
      PACKETSTORM:140070      7.8     https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
      PACKETSTORM:101052      7.8     https://vulners.com/packetstorm/PACKETSTORM:101052      *EXPLOIT*
      EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985    7.8     https://vulners.com/exploitpack/EXPLOITPACK:71D51B69AA2D3A74753
      EXPLOITPACK:67F6569F63A082199721C069C852BBD7    7.8     https://vulners.com/exploitpack/EXPLOITPACK:67F6569F63A08219972
      EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    7.8     https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE293
      EDB-ID:24450    7.8     https://vulners.com/exploitdb/EDB-ID:24450      *EXPLOIT*
      EDB-ID:15215    7.8     https://vulners.com/exploitdb/EDB-ID:15215      *EXPLOIT*
      CVE-2020-15778  7.8     https://vulners.com/cve/CVE-2020-15778
      CVE-2016-10012  7.8     https://vulners.com/cve/CVE-2016-10012
      CVE-2015-8325   7.8     https://vulners.com/cve/CVE-2015-8325
      1337DAY-ID-26494        7.8     https://vulners.com/zdt/1337DAY-ID-26494        *EXPLOIT*
      SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *EXPLOIT*
      SSV:61450       7.5     https://vulners.com/seebug/SSV:61450    *EXPLOIT*
      PACKETSTORM:173661      7.5     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
      F0979183-AE88-53B4-86CF-3AF0523F3807    7.5     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807
      EDB-ID:40888    7.5     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
      CVE-2016-6515   7.5     https://vulners.com/cve/CVE-2016-6515
      CVE-2016-10708  7.5     https://vulners.com/cve/CVE-2016-10708
      CVE-2014-1692   7.5     https://vulners.com/cve/CVE-2014-1692
      CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
      1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-26576        *EXPLOIT*
      CVE-2016-10009  7.3     https://vulners.com/cve/CVE-2016-10009
      SSV:92582       7.2     https://vulners.com/seebug/SSV:92582    *EXPLOIT*
      CVE-2016-10010  7.0     https://vulners.com/cve/CVE-2016-10010
      SSV:92580       6.9     https://vulners.com/seebug/SSV:92580    *EXPLOIT*
      CVE-2015-6564   6.9     https://vulners.com/cve/CVE-2015-6564
      1337DAY-ID-26577        6.9     https://vulners.com/zdt/1337DAY-ID-26577        *EXPLOIT*
      EDB-ID:46516    6.8     https://vulners.com/exploitdb/EDB-ID:46516      *EXPLOIT*
      EDB-ID:46193    6.8     https://vulners.com/exploitdb/EDB-ID:46193      *EXPLOIT*
      CVE-2019-6110   6.8     https://vulners.com/cve/CVE-2019-6110
      CVE-2019-6109   6.8     https://vulners.com/cve/CVE-2019-6109
      C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3    6.8     https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3
      10213DBE-F683-58BB-B6D3-353173626207    6.8     https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207
      CVE-2023-51385  6.5     https://vulners.com/cve/CVE-2023-51385
      CVE-2008-1657   6.5     https://vulners.com/cve/CVE-2008-1657
      EDB-ID:40858    6.4     https://vulners.com/exploitdb/EDB-ID:40858      *EXPLOIT*
      EDB-ID:40119    6.4     https://vulners.com/exploitdb/EDB-ID:40119      *EXPLOIT*
      EDB-ID:39569    6.4     https://vulners.com/exploitdb/EDB-ID:39569      *EXPLOIT*
      CVE-2016-3115   6.4     https://vulners.com/cve/CVE-2016-3115
      EDB-ID:40136    5.9     https://vulners.com/exploitdb/EDB-ID:40136      *EXPLOIT*
      EDB-ID:40113    5.9     https://vulners.com/exploitdb/EDB-ID:40113      *EXPLOIT*
      CVE-2023-48795  5.9     https://vulners.com/cve/CVE-2023-48795
      CVE-2019-6111   5.9     https://vulners.com/cve/CVE-2019-6111
      CVE-2016-6210   5.9     https://vulners.com/cve/CVE-2016-6210
      SSV:61911       5.8     https://vulners.com/seebug/SSV:61911    *EXPLOIT*
      EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8     https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84
      EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8     https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9
      CVE-2014-2653   5.8     https://vulners.com/cve/CVE-2014-2653
      1337DAY-ID-32328        5.8     https://vulners.com/zdt/1337DAY-ID-32328        *EXPLOIT*
      1337DAY-ID-32009        5.8     https://vulners.com/zdt/1337DAY-ID-32009        *EXPLOIT*
      SSV:91041       5.5     https://vulners.com/seebug/SSV:91041    *EXPLOIT*
      PACKETSTORM:140019      5.5     https://vulners.com/packetstorm/PACKETSTORM:140019      *EXPLOIT*
      PACKETSTORM:136234      5.5     https://vulners.com/packetstorm/PACKETSTORM:136234      *EXPLOIT*
      EXPLOITPACK:F92411A645D85F05BDBD274FD222226F    5.5     https://vulners.com/exploitpack/EXPLOITPACK:F92411A645D85F05BDB
      EXPLOITPACK:9F2E746846C3C623A27A441281EAD138    5.5     https://vulners.com/exploitpack/EXPLOITPACK:9F2E746846C3C623A27
      EXPLOITPACK:1902C998CBF9154396911926B4C3B330    5.5     https://vulners.com/exploitpack/EXPLOITPACK:1902C998CBF91543969
      CVE-2016-10011  5.5     https://vulners.com/cve/CVE-2016-10011
      1337DAY-ID-25388        5.5     https://vulners.com/zdt/1337DAY-ID-25388        *EXPLOIT*
      PACKETSTORM:181223      5.3     https://vulners.com/packetstorm/PACKETSTORM:181223      *EXPLOIT*
      MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-        5.3     https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_EN
      EDB-ID:45939    5.3     https://vulners.com/exploitdb/EDB-ID:45939      *EXPLOIT*
      EDB-ID:45233    5.3     https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
      CVE-2018-20685  5.3     https://vulners.com/cve/CVE-2018-20685
      CVE-2018-15473  5.3     https://vulners.com/cve/CVE-2018-15473
      CVE-2017-15906  5.3     https://vulners.com/cve/CVE-2017-15906
      CVE-2016-20012  5.3     https://vulners.com/cve/CVE-2016-20012
      SSV:60656       5.0     https://vulners.com/seebug/SSV:60656    *EXPLOIT*
      SSH_ENUM        5.0     https://vulners.com/canvas/SSH_ENUM     *EXPLOIT*
      PACKETSTORM:150621      5.0     https://vulners.com/packetstorm/PACKETSTORM:150621      *EXPLOIT*
      EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0    5.0     https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C
```

```
        EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283    5.0     https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B
        CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2010-5107
        1337DAY-ID-31730        5.0     https://vulners.com/zdt/1337DAY-ID-31730        *EXPLOIT*
        CVE-2014-2532   4.9     https://vulners.com/cve/CVE-2014-2532
        EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF    4.3     https://vulners.com/exploitpack/EXPLOITPACK:802AF3229492E147A5F
        EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF    4.3     https://vulners.com/exploitpack/EXPLOITPACK:5652DDAA7FE452E19AC
        CVE-2015-5352   4.3     https://vulners.com/cve/CVE-2015-5352
        1337DAY-ID-25440        4.3     https://vulners.com/zdt/1337DAY-ID-25440        *EXPLOIT*
        1337DAY-ID-25438        4.3     https://vulners.com/zdt/1337DAY-ID-25438        *EXPLOIT*
        CVE-2010-4755   4.0     https://vulners.com/cve/CVE-2010-4755
        CVE-2021-36368  3.7     https://vulners.com/cve/CVE-2021-36368
        CVE-2012-0814   3.5     https://vulners.com/cve/CVE-2012-0814
        CVE-2011-5000   3.5     https://vulners.com/cve/CVE-2011-5000
        SSV:92581       2.1     https://vulners.com/seebug/SSV:92581    *EXPLOIT*
        CVE-2011-4327   2.1     https://vulners.com/cve/CVE-2011-4327
        CVE-2015-6563   1.9     https://vulners.com/cve/CVE-2015-6563
        CVE-2008-3259   1.2     https://vulners.com/cve/CVE-2008-3259
        PACKETSTORM:151227      0.0     https://vulners.com/packetstorm/PACKETSTORM:151227      *EXPLOIT*
        PACKETSTORM:140261      0.0     https://vulners.com/packetstorm/PACKETSTORM:140261      *EXPLOIT*
        PACKETSTORM:138006      0.0     https://vulners.com/packetstorm/PACKETSTORM:138006      *EXPLOIT*
        PACKETSTORM:137942      0.0     https://vulners.com/packetstorm/PACKETSTORM:137942      *EXPLOIT*
        EDB-ID:45210    0.0     https://vulners.com/exploitdb/EDB-ID:45210      *EXPLOIT*
        EDB-ID:40963    0.0     https://vulners.com/exploitdb/EDB-ID:40963      *EXPLOIT*
        EDB-ID:40962    0.0     https://vulners.com/exploitdb/EDB-ID:40962      *EXPLOIT*
        1337DAY-ID-30937        0.0     https://vulners.com/zdt/1337DAY-ID-30937        *EXPLOIT*
        1337DAY-ID-26468        0.0     https://vulners.com/zdt/1337DAY-ID-26468        *EXPLOIT*
        1337DAY-ID-25391        0.0     https://vulners.com/zdt/1337DAY-ID-25391        *EXPLOIT*
```

	ssh-run	Failed to specify credentials and command to run.		
	ssh2-enum-algos	kex_algorithms: (4) server_host_key_algorithms: (2) encryption_algorithms: (13) mac_algorithms: (7) compression_algorithms: (2)		
	banner	SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1		
	ssh-auth-methods	Supported authentication methods: publickey password		
23	tcp	open	telnet	syn-a
	tso-brute	ERROR: Script execution failed (use -d to debug)		
	banner	\xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'		
	vtam-enum	Not VTAM or 'logon applid' command not accepted. Try with script arg 'vtam-enum.macros=true'		
	telnet-brute	Accounts: No valid accounts found Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0 ERROR: The service seems to have failed or is heavily firewalled...		
	tso-enum	ERROR: Script execution failed (use -d to debug)		
25	tcp	open	smtp	syn-a
	smtp-commands	metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN		
	smtp-open-relay	Server doesn't seem to be an open relay, all tests failed		
	banner	220 metasploitable.localdomain ESMTP Postfix (Ubuntu)		
	smtp-vuln-cve2010-4344	The SMTP server is not Exim: NOT VULNERABLE		
	smtp-enum-users	Method RCPT returned a unhandled status code.		
53	tcp	open	domain	syn-a
	vulners	cpe:/a:isc:bind:9.4.2: SSV:2853 10.0 https://vulners.com/seebug/SSV:2853 *EXPLOIT* CVE-2008-0122 10.0 https://vulners.com/cve/CVE-2008-0122 95499236-C9FE-56A6-9D7D-E943A24B633A 10.0 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A 2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0 https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A CVE-2021-25216 9.8 https://vulners.com/cve/CVE-2021-25216 CVE-2020-8616 8.6 https://vulners.com/cve/CVE-2020-8616 CVE-2016-1286 8.6 https://vulners.com/cve/CVE-2016-1286 SSV:60184 8.5 https://vulners.com/seebug/SSV:60184 *EXPLOIT* CVE-2012-1667 8.5 https://vulners.com/cve/CVE-2012-1667 SSV:60292 7.8 https://vulners.com/seebug/SSV:60292 *EXPLOIT* PACKETSTORM:180552 7.8 https://vulners.com/packetstorm/PACKETSTORM:180552 *EXPLOIT* PACKETSTORM:138960 7.8 https://vulners.com/packetstorm/PACKETSTORM:138960 *EXPLOIT* PACKETSTORM:132926 7.8 https://vulners.com/packetstorm/PACKETSTORM:132926 *EXPLOIT* MSF:AUXILIARY-DOS-DNS-BIND_TKEY- 7.8 https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TKEY- *EXPLOI EXPLOITPACK:BE4F638B632EA0754155A27ECC4B3D3F 7.8 https://vulners.com/exploitpack/EXPLOITPACK:BE4F638B632EA075415 EXPLOITPACK:46DEBFAC850194C04C54F93E0DFF5F4F 7.8 https://vulners.com/exploitpack/EXPLOITPACK:46DEBFAC850194C04C5 EXPLOITPACK:09762DB0197BBAAAB6FC79F24F0D2A74 7.8 https://vulners.com/exploitpack/EXPLOITPACK:09762DB0197BBAAAB6F EDB-ID:42121 7.8 https://vulners.com/exploitdb/EDB-ID:42121 *EXPLOIT* EDB-ID:37723 7.8 https://vulners.com/exploitdb/EDB-ID:37723 *EXPLOIT*		

```
EDB-ID:37721    7.8     https://vulners.com/exploitdb/EDB-ID:37721      *EXPLOIT*
CVE-2017-3141   7.8     https://vulners.com/cve/CVE-2017-3141
CVE-2015-5722   7.8     https://vulners.com/cve/CVE-2015-5722
CVE-2015-5477   7.8     https://vulners.com/cve/CVE-2015-5477
CVE-2014-8500   7.8     https://vulners.com/cve/CVE-2014-8500
CVE-2012-5166   7.8     https://vulners.com/cve/CVE-2012-5166
CVE-2012-4244   7.8     https://vulners.com/cve/CVE-2012-4244
CVE-2012-3817   7.8     https://vulners.com/cve/CVE-2012-3817
CVE-2008-4163   7.8     https://vulners.com/cve/CVE-2008-4163
1337DAY-ID-25325        7.8     https://vulners.com/zdt/1337DAY-ID-25325        *EXPLOIT*
1337DAY-ID-23970        7.8     https://vulners.com/zdt/1337DAY-ID-23970        *EXPLOIT*
1337DAY-ID-23960        7.8     https://vulners.com/zdt/1337DAY-ID-23960        *EXPLOIT*
1337DAY-ID-23948        7.8     https://vulners.com/zdt/1337DAY-ID-23948        *EXPLOIT*
CVE-2010-0382   7.6     https://vulners.com/cve/CVE-2010-0382
PACKETSTORM:180551      7.5     https://vulners.com/packetstorm/PACKETSTORM:180551      *EXPLOIT*
PACKETSTORM:180550      7.5     https://vulners.com/packetstorm/PACKETSTORM:180550      *EXPLOIT*
MSF:AUXILIARY-DOS-DNS-BIND_TSIG_BADTIME-        7.5     https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TSIG_
MSF:AUXILIARY-DOS-DNS-BIND_TSIG-        7.5     https://vulners.com/metasploit/MSF:AUXILIARY-DOS-DNS-BIND_TSIG- *EXPLOI
EDB-ID:40453    7.5     https://vulners.com/exploitdb/EDB-ID:40453      *EXPLOIT*
CVE-2023-50387  7.5     https://vulners.com/cve/CVE-2023-50387
CVE-2023-3341   7.5     https://vulners.com/cve/CVE-2023-3341
CVE-2021-25215  7.5     https://vulners.com/cve/CVE-2021-25215
CVE-2020-8617   7.5     https://vulners.com/cve/CVE-2020-8617
CVE-2017-3145   7.5     https://vulners.com/cve/CVE-2017-3145
CVE-2017-3143   7.5     https://vulners.com/cve/CVE-2017-3143
CVE-2016-9444   7.5     https://vulners.com/cve/CVE-2016-9444
CVE-2016-9131   7.5     https://vulners.com/cve/CVE-2016-9131
CVE-2016-8864   7.5     https://vulners.com/cve/CVE-2016-8864
CVE-2016-2848   7.5     https://vulners.com/cve/CVE-2016-2848
CVE-2016-2776   7.5     https://vulners.com/cve/CVE-2016-2776
CVE-2009-0265   7.5     https://vulners.com/cve/CVE-2009-0265
BB688FBF-CEE2-5DD1-8561-8F76501DE2D4    7.5     https://vulners.com/githubexploit/BB688FBF-CEE2-5DD1-8561-8F76501DE2D4
5EFDF373-FBD1-5C09-A612-00ADBFE574CF    7.5     https://vulners.com/githubexploit/5EFDF373-FBD1-5C09-A612-00ADBFE574CF
1337DAY-ID-34485        7.5     https://vulners.com/zdt/1337DAY-ID-34485        *EXPLOIT*
EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2    7.2     https://vulners.com/exploitpack/EXPLOITPACK:D6DDF5E24DE171DAAD7
CVE-2015-8461   7.1     https://vulners.com/cve/CVE-2015-8461
CVE-2015-5986   7.1     https://vulners.com/cve/CVE-2015-5986
CVE-2015-8705   7.0     https://vulners.com/cve/CVE-2015-8705
CVE-2016-1285   6.8     https://vulners.com/cve/CVE-2016-1285
CVE-2009-0025   6.8     https://vulners.com/cve/CVE-2009-0025
CVE-2020-8622   6.5     https://vulners.com/cve/CVE-2020-8622
CVE-2018-5741   6.5     https://vulners.com/cve/CVE-2018-5741
CVE-2016-6170   6.5     https://vulners.com/cve/CVE-2016-6170
CVE-2015-8704   6.5     https://vulners.com/cve/CVE-2015-8704
CVE-2010-3614   6.4     https://vulners.com/cve/CVE-2010-3614
CVE-2016-2775   5.9     https://vulners.com/cve/CVE-2016-2775
SSV:4636        5.8     https://vulners.com/seebug/SSV:4636     *EXPLOIT*
CVE-2022-2795   5.3     https://vulners.com/cve/CVE-2022-2795
CVE-2021-25219  5.3     https://vulners.com/cve/CVE-2021-25219
CVE-2017-3142   5.3     https://vulners.com/cve/CVE-2017-3142
SSV:30099       5.0     https://vulners.com/seebug/SSV:30099    *EXPLOIT*
SSV:20595       5.0     https://vulners.com/seebug/SSV:20595    *EXPLOIT*
PACKETSTORM:157836      5.0     https://vulners.com/packetstorm/PACKETSTORM:157836      *EXPLOIT*
FBC03933-7A65-52F3-83F4-4B2253A490B6    5.0     https://vulners.com/githubexploit/FBC03933-7A65-52F3-83F4-4B2253A490B6
CVE-2015-8000   5.0     https://vulners.com/cve/CVE-2015-8000
CVE-2012-1033   5.0     https://vulners.com/cve/CVE-2012-1033
CVE-2011-4313   5.0     https://vulners.com/cve/CVE-2011-4313
CVE-2011-1910   5.0     https://vulners.com/cve/CVE-2011-1910
SSV:11919       4.3     https://vulners.com/seebug/SSV:11919    *EXPLOIT*
CVE-2010-3762   4.3     https://vulners.com/cve/CVE-2010-3762
CVE-2010-0097   4.3     https://vulners.com/cve/CVE-2010-0097
CVE-2009-0696   4.3     https://vulners.com/cve/CVE-2009-0696
CVE-2010-0290   4.0     https://vulners.com/cve/CVE-2010-0290
SSV:14986       2.6     https://vulners.com/seebug/SSV:14986    *EXPLOIT*
CVE-2009-4022   2.6     https://vulners.com/cve/CVE-2009-4022
PACKETSTORM:142800      0.0     https://vulners.com/packetstorm/PACKETSTORM:142800      *EXPLOIT*
EDB-ID:9300     0.0     https://vulners.com/exploitdb/EDB-ID:9300       *EXPLOIT*
EDB-ID:48521    0.0     https://vulners.com/exploitdb/EDB-ID:48521      *EXPLOIT*
1337DAY-ID-27896        0.0     https://vulners.com/zdt/1337DAY-ID-27896        *EXPLOIT*
```

	dns-fuzz	Server didn't response to our probe, can't fuzz		
	dns-nsid	bind.version: 9.4.2		
	dns-nsec-enum	Can't determine domain for host 192.168.50.100; use dns-nsec-enum.domains script arg.		
	dns-nsec3-enum	Can't determine domain for host 192.168.50.100; use dns-nsec3-enum.domains script arg.		
80	tcp	open	http	syn-ac
	http-xssed	No previously reported XSS vuln.		
	citrix-brute-xml	FAILED: No domain specified (use ntdomain argument)		
	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-feed	Couldn't find any feeds.		

http-slowloris

```
false
```

http-php-version

```
Versions from logo query (less accurate): 5.1.3 - 5.1.6, 5.2.0 - 5.2.17
Versions from credits query (more accurate): 5.2.3 - 5.2.5, 5.2.6RC3
Version from header x-powered-by: PHP/5.2.4-2ubuntu5.10
```

http-grep

```
  (1) http://192.168.50.100:80/dav/:
    (1) ip:
      + 192.168.50.100
  (1) http://192.168.50.100:80/mutillidae/?page=credits.php:
    (1) email:
      + mutillidae-development@gmail.com
```

http-trace

```
TRACE is enabled
```

http-security-headers

http-vuln-cve2017-1001000

```
ERROR: Script execution failed (use -d to debug)
```

http-errors

```
Couldn't find any error pages.
```

http-fetch

```
Please enter the complete path of the directory to save data in.
```

http-headers

```
  Date: Fri, 27 Sep 2024 19:48:45 GMT
  Server: Apache/2.2.8 (Ubuntu) DAV/2
  X-Powered-By: PHP/5.2.4-2ubuntu5.10
  Connection: close
  Content-Type: text/html

  (Request type: HEAD)
```

http-vhosts

```
128 names had status 200
```

http-apache-negotiation

```
mod_negotiation enabled.
```

vulners

```
  cpe:/a:apache:http_server:2.2.8:
        SSV:69341       10.0    https://vulners.com/seebug/SSV:69341    *EXPLOIT*
        SSV:19282       10.0    https://vulners.com/seebug/SSV:19282    *EXPLOIT*
        SSV:19236       10.0    https://vulners.com/seebug/SSV:19236    *EXPLOIT*
        PACKETSTORM:86964       10.0    https://vulners.com/packetstorm/PACKETSTORM:86964       *EXPLOIT*
        PACKETSTORM:180533      10.0    https://vulners.com/packetstorm/PACKETSTORM:180533      *EXPLOIT*
        MSF:AUXILIARY-DOS-HTTP-APACHE_MOD_ISAPI-        10.0    https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_MO
        FF2EF58E-53AA-5B60-9EA1-4B5C29647395    10.0    https://vulners.com/githubexploit/FF2EF58E-53AA-5B60-9EA1-4B5C29647395
        EXPLOITPACK:30ED468EC8BD5B71B2CB93825A852B80    10.0    https://vulners.com/exploitpack/EXPLOITPACK:30ED468EC8BD5B71B2C
        EDB-ID:14288    10.0    https://vulners.com/exploitdb/EDB-ID:14288      *EXPLOIT*
        EDB-ID:11650    10.0    https://vulners.com/exploitdb/EDB-ID:11650      *EXPLOIT*
        CVE-2010-0425   10.0    https://vulners.com/cve/CVE-2010-0425
        C94CBDE1-4CC5-5C06-9D18-23CAB216705E    10.0    https://vulners.com/githubexploit/C94CBDE1-4CC5-5C06-9D18-23CAB216705E
        95499236-C9FE-56A6-9D7D-E943A24B633A    10.0    https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A
        2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0    https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A
        PACKETSTORM:181114      9.8     https://vulners.com/packetstorm/PACKETSTORM:181114      *EXPLOIT*
        MSF:EXPLOIT-MULTI-HTTP-APACHE_NORMALIZE_PATH_RCE-       9.8     https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-HTTP-A
        MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH-       9.8     https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HT
        F9C0CD4B-3B60-5720-AE7A-7CC31DB839C5    9.8     https://vulners.com/githubexploit/F9C0CD4B-3B60-5720-AE7A-7CC31DB839C5
        F607361B-6369-5DF5-9B29-E90FA29DC565    9.8     https://vulners.com/githubexploit/F607361B-6369-5DF5-9B29-E90FA29DC565
        F41EE867-4E63-5259-9DF0-745881884D04    9.8     https://vulners.com/githubexploit/F41EE867-4E63-5259-9DF0-745881884D04
        EDB-ID:51193    9.8     https://vulners.com/exploitdb/EDB-ID:51193      *EXPLOIT*
        EDB-ID:50512    9.8     https://vulners.com/exploitdb/EDB-ID:50512      *EXPLOIT*
        EDB-ID:50446    9.8     https://vulners.com/exploitdb/EDB-ID:50446      *EXPLOIT*
        EDB-ID:50406    9.8     https://vulners.com/exploitdb/EDB-ID:50406      *EXPLOIT*
        E796A40A-8A8E-59D1-93FB-78EF4D8B7FA6    9.8     https://vulners.com/githubexploit/E796A40A-8A8E-59D1-93FB-78EF4D8B7FA6
        D10426F3-DF82-5439-AC3E-6CA0A1365A09    9.8     https://vulners.com/githubexploit/D10426F3-DF82-5439-AC3E-6CA0A1365A09
        D0368327-F989-5557-A5C6-0D9ACDB4E72F    9.8     https://vulners.com/githubexploit/D0368327-F989-5557-A5C6-0D9ACDB4E72F
        CVE-2024-38476  9.8     https://vulners.com/cve/CVE-2024-38476
        CVE-2024-38474  9.8     https://vulners.com/cve/CVE-2024-38474
        CVE-2023-25690  9.8     https://vulners.com/cve/CVE-2023-25690
        CVE-2022-31813  9.8     https://vulners.com/cve/CVE-2022-31813
        CVE-2022-23943  9.8     https://vulners.com/cve/CVE-2022-23943
        CVE-2022-22720  9.8     https://vulners.com/cve/CVE-2022-22720
        CVE-2021-44790  9.8     https://vulners.com/cve/CVE-2021-44790
        CVE-2021-42013  9.8     https://vulners.com/cve/CVE-2021-42013
        CVE-2021-39275  9.8     https://vulners.com/cve/CVE-2021-39275
        CVE-2021-26691  9.8     https://vulners.com/cve/CVE-2021-26691
        CVE-2018-1312   9.8     https://vulners.com/cve/CVE-2018-1312
        CVE-2017-7679   9.8     https://vulners.com/cve/CVE-2017-7679
        CVE-2017-3169   9.8     https://vulners.com/cve/CVE-2017-3169
        CVE-2017-3167   9.8     https://vulners.com/cve/CVE-2017-3167
        CC15AE65-B697-525A-AF4B-38B1501CAB49    9.8     https://vulners.com/githubexploit/CC15AE65-B697-525A-AF4B-38B1501CAB49
        C879EE66-6B75-5EC8-AA68-08693C6CCAD1    9.8     https://vulners.com/githubexploit/C879EE66-6B75-5EC8-AA68-08693C6CCAD1
        C5A61CC6-919E-58B4-8FBB-0198654A7FC8    9.8     https://vulners.com/githubexploit/C5A61CC6-919E-58B4-8FBB-0198654A7FC8
        BF9B0898-784E-5B5E-9505-430B58C1E6B8    9.8     https://vulners.com/githubexploit/BF9B0898-784E-5B5E-9505-430B58C1E6B8
        B02819DB-1481-56C4-BD09-6B4574297109    9.8     https://vulners.com/githubexploit/B02819DB-1481-56C4-BD09-6B4574297109
        ACD5A7F2-FDB2-5859-8D23-3266A1AF6795    9.8     https://vulners.com/githubexploit/ACD5A7F2-FDB2-5859-8D23-3266A1AF6795
        A90ABEAD-13A8-5F09-8A19-6D9D2D804F05    9.8     https://vulners.com/githubexploit/A90ABEAD-13A8-5F09-8A19-6D9D2D804F05
        A8616E5E-04F8-56D8-ACB4-32FDF7F66EED    9.8     https://vulners.com/githubexploit/A8616E5E-04F8-56D8-ACB4-32FDF7F66EED
        A2D97DCC-04C2-5CB1-921F-709AA8D7FD9A    9.8     https://vulners.com/githubexploit/A2D97DCC-04C2-5CB1-921F-709AA8D7FD9A
        9B4F4E4A-CFDF-5847-805F-C0BAE809DBD5    9.8     https://vulners.com/githubexploit/9B4F4E4A-CFDF-5847-805F-C0BAE809DBD5
        907F28D0-5906-51C7-BAA3-FEBD5E878801    9.8     https://vulners.com/githubexploit/907F28D0-5906-51C7-BAA3-FEBD5E878801
        8A57FAF6-FC91-52D1-84E0-4CBBAD3F9677    9.8     https://vulners.com/githubexploit/8A57FAF6-FC91-52D1-84E0-4CBBAD3F9677
        88EB009A-EEFF-52B7-811D-A8A8C8DE8C81    9.8     https://vulners.com/githubexploit/88EB009A-EEFF-52B7-811D-A8A8C8DE8C81
        8713FD59-264B-5FD7-8429-3251AB5AB3B8    9.8     https://vulners.com/githubexploit/8713FD59-264B-5FD7-8429-3251AB5AB3B8
```

```
866E26E3-759B-526D-ABB5-206B2A1AC3EE    9.8     https://vulners.com/githubexploit/866E26E3-759B-526D-ABB5-206B2A1AC3EE
86360765-0B1A-5D73-A805-BAE8F1B5D16D    9.8     https://vulners.com/githubexploit/86360765-0B1A-5D73-A805-BAE8F1B5D16D
831E1114-13D1-54EF-BDE4-F655114CDC29    9.8     https://vulners.com/githubexploit/831E1114-13D1-54EF-BDE4-F655114CDC29
805E6B24-8DF9-51D8-8DF6-6658161F96EA    9.8     https://vulners.com/githubexploit/805E6B24-8DF9-51D8-8DF6-6658161F96EA
7E615961-3792-5896-94FA-1F9D494ACB36    9.8     https://vulners.com/githubexploit/7E615961-3792-5896-94FA-1F9D494ACB36
78787F63-0356-51EC-B32A-B9BD114431C3    9.8     https://vulners.com/githubexploit/78787F63-0356-51EC-B32A-B9BD114431C3
6CAA7558-723B-5286-9840-4DF4EB48E0AF    9.8     https://vulners.com/githubexploit/6CAA7558-723B-5286-9840-4DF4EB48E0AF
6A0A657E-8300-5312-99CE-E11F460B1DBF    9.8     https://vulners.com/githubexploit/6A0A657E-8300-5312-99CE-E11F460B1DBF
64D31BF1-F977-51EC-AB1C-6693CA6B58F3    9.8     https://vulners.com/githubexploit/64D31BF1-F977-51EC-AB1C-6693CA6B58F3
61075B23-F713-537A-9B84-7EB9B96CF228    9.8     https://vulners.com/githubexploit/61075B23-F713-537A-9B84-7EB9B96CF228
5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9    9.8     https://vulners.com/githubexploit/5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9
5312D04F-9490-5472-84FA-86B3BBDC8928    9.8     https://vulners.com/githubexploit/5312D04F-9490-5472-84FA-86B3BBDC8928
52E13088-9643-5E81-B0A0-B7478BCF1F2C    9.8     https://vulners.com/githubexploit/52E13088-9643-5E81-B0A0-B7478BCF1F2C
495E99E5-C1B0-52C1-9218-384D04161BE4    9.8     https://vulners.com/githubexploit/495E99E5-C1B0-52C1-9218-384D04161BE4
44E43BB7-6255-58E7-99C7-C3B84645D497    9.8     https://vulners.com/githubexploit/44E43BB7-6255-58E7-99C7-C3B84645D497
3F17CA20-788F-5C45-88B3-E12DB2979B7B    9.8     https://vulners.com/githubexploit/3F17CA20-788F-5C45-88B3-E12DB2979B7B
37634050-FDDF-571A-90BB-C8109824B38D    9.8     https://vulners.com/githubexploit/37634050-FDDF-571A-90BB-C8109824B38D
30293CDA-FDB1-5FAF-9622-88427267F204    9.8     https://vulners.com/githubexploit/30293CDA-FDB1-5FAF-9622-88427267F204
2B3110E1-BEA0-5DB8-93AD-1682230F3E19    9.8     https://vulners.com/githubexploit/2B3110E1-BEA0-5DB8-93AD-1682230F3E19
22DCCD26-B68C-5905-BAC2-71D10DE3F123    9.8     https://vulners.com/githubexploit/22DCCD26-B68C-5905-BAC2-71D10DE3F123
2108729F-1E99-54EF-9A4B-47299FD89FF2    9.8     https://vulners.com/githubexploit/2108729F-1E99-54EF-9A4B-47299FD89FF2
1C39E10A-4A38-5228-8334-2A5F8AAB7FC3    9.8     https://vulners.com/githubexploit/1C39E10A-4A38-5228-8334-2A5F8AAB7FC3
1337DAY-ID-39214        9.8     https://vulners.com/zdt/1337DAY-ID-39214        *EXPLOIT*
1337DAY-ID-37777        9.8     https://vulners.com/zdt/1337DAY-ID-37777        *EXPLOIT*
1337DAY-ID-36952        9.8     https://vulners.com/zdt/1337DAY-ID-36952        *EXPLOIT*
11813536-2AFF-5EA4-B09F-E9EB340DDD26    9.8     https://vulners.com/githubexploit/11813536-2AFF-5EA4-B09F-E9EB340DDD26
0C47BCF2-EA6F-5613-A6E8-B707D64155DE    9.8     https://vulners.com/githubexploit/0C47BCF2-EA6F-5613-A6E8-B707D64155DE
0AA6A425-25B1-5D2A-ABA1-2933D3E1DC56    9.8     https://vulners.com/githubexploit/0AA6A425-25B1-5D2A-ABA1-2933D3E1DC56
07AA70EA-C34E-5F66-9510-7C265093992A    9.8     https://vulners.com/githubexploit/07AA70EA-C34E-5F66-9510-7C265093992A
CVE-2024-38475  9.1     https://vulners.com/cve/CVE-2024-38475
CVE-2022-28615  9.1     https://vulners.com/cve/CVE-2022-28615
CVE-2022-22721  9.1     https://vulners.com/cve/CVE-2022-22721
CVE-2017-9788   9.1     https://vulners.com/cve/CVE-2017-9788
0486EBEE-F207-570A-9AD8-33269E72220A    9.1     https://vulners.com/githubexploit/0486EBEE-F207-570A-9AD8-33269E72220A
CVE-2022-36760  9.0     https://vulners.com/cve/CVE-2022-36760
CVE-2021-40438  9.0     https://vulners.com/cve/CVE-2021-40438
AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C    9.0     https://vulners.com/githubexploit/AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C
8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2    9.0     https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2
7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2    9.0     https://vulners.com/githubexploit/7F48C6CF-47B2-5AF9-B6FD-1735FB2A95B2
4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332    9.0     https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332
4373C92A-2755-5538-9C91-0469C995AA9B    9.0     https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B
36618CA8-9316-59CA-B748-82F15F407C4F    9.0     https://vulners.com/githubexploit/36618CA8-9316-59CA-B748-82F15F407C4F
CVE-2021-44224  8.2     https://vulners.com/cve/CVE-2021-44224
B0A9E5E8-7CCC-5984-9922-A89F11D6BF38    8.2     https://vulners.com/githubexploit/B0A9E5E8-7CCC-5984-9922-A89F11D6BF38
CVE-2024-38473  8.1     https://vulners.com/cve/CVE-2024-38473
CVE-2016-5387   8.1     https://vulners.com/cve/CVE-2016-5387
249A954E-0189-5182-AE95-31C866A057E1    8.1     https://vulners.com/githubexploit/249A954E-0189-5182-AE95-31C866A057E1
23079A70-8B37-56D2-9D37-F638EBF7F8B5    8.1     https://vulners.com/githubexploit/23079A70-8B37-56D2-9D37-F638EBF7F8B5
SSV:72403       7.8     https://vulners.com/seebug/SSV:72403    *EXPLOIT*
SSV:2820        7.8     https://vulners.com/seebug/SSV:2820     *EXPLOIT*
SSV:26043       7.8     https://vulners.com/seebug/SSV:26043    *EXPLOIT*
SSV:20899       7.8     https://vulners.com/seebug/SSV:20899    *EXPLOIT*
SSV:11569       7.8     https://vulners.com/seebug/SSV:11569    *EXPLOIT*
PACKETSTORM:180517      7.8     https://vulners.com/packetstorm/PACKETSTORM:180517      *EXPLOIT*
PACKETSTORM:126851      7.8     https://vulners.com/packetstorm/PACKETSTORM:126851      *EXPLOIT*
PACKETSTORM:123527      7.8     https://vulners.com/packetstorm/PACKETSTORM:123527      *EXPLOIT*
PACKETSTORM:122962      7.8     https://vulners.com/packetstorm/PACKETSTORM:122962      *EXPLOIT*
MSF:AUXILIARY-DOS-HTTP-APACHE_RANGE_DOS-        7.8     https://vulners.com/metasploit/MSF:AUXILIARY-DOS-HTTP-APACHE_RA
EXPLOITPACK:186B5FCF5C57B52642E62C06BABC6F83    7.8     https://vulners.com/exploitpack/EXPLOITPACK:186B5FCF5C57B52642E
EDB-ID:18221    7.8     https://vulners.com/exploitdb/EDB-ID:18221      *EXPLOIT*
CVE-2011-3192   7.8     https://vulners.com/cve/CVE-2011-3192
1337DAY-ID-21170        7.8     https://vulners.com/zdt/1337DAY-ID-21170        *EXPLOIT*
SSV:12673       7.5     https://vulners.com/seebug/SSV:12673    *EXPLOIT*
SSV:12626       7.5     https://vulners.com/seebug/SSV:12626    *EXPLOIT*
PACKETSTORM:181038      7.5     https://vulners.com/packetstorm/PACKETSTORM:181038      *EXPLOIT*
PACKETSTORM:176334      7.5     https://vulners.com/packetstorm/PACKETSTORM:176334      *EXPLOIT*
PACKETSTORM:171631      7.5     https://vulners.com/packetstorm/PACKETSTORM:171631      *EXPLOIT*
PACKETSTORM:164941      7.5     https://vulners.com/packetstorm/PACKETSTORM:164941      *EXPLOIT*
PACKETSTORM:164629      7.5     https://vulners.com/packetstorm/PACKETSTORM:164629      *EXPLOIT*
PACKETSTORM:164609      7.5     https://vulners.com/packetstorm/PACKETSTORM:164609      *EXPLOIT*
MSF:AUXILIARY-SCANNER-HTTP-APACHE_OPTIONSBLEED- 7.5     https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACH
FF610CB4-801A-5D1D-9AC9-ADFC287C8482    7.5     https://vulners.com/githubexploit/FF610CB4-801A-5D1D-9AC9-ADFC287C8482
FDF4BBB1-979C-5320-95EA-9EC7EB064D72    7.5     https://vulners.com/githubexploit/FDF4BBB1-979C-5320-95EA-9EC7EB064D72
FCAF01A0-F921-5DB1-BBC5-850EC2DC5C46    7.5     https://vulners.com/githubexploit/FCAF01A0-F921-5DB1-BBC5-850EC2DC5C46
F8A7DE57-8F14-5B3C-A102-D546BDD8D2B8    7.5     https://vulners.com/githubexploit/F8A7DE57-8F14-5B3C-A102-D546BDD8D2B8
F7F6E599-CEF4-5E03-8E10-FE18C4101E38    7.5     https://vulners.com/githubexploit/F7F6E599-CEF4-5E03-8E10-FE18C4101E38
EDB-ID:50383    7.5     https://vulners.com/exploitdb/EDB-ID:50383      *EXPLOIT*
EDB-ID:42745    7.5     https://vulners.com/exploitdb/EDB-ID:42745      *EXPLOIT*
ECC3E825-EE29-59D3-BE28-1B30DB15940E    7.5     https://vulners.com/githubexploit/ECC3E825-EE29-59D3-BE28-1B30DB15940E
E81474F6-6DDC-5FC2-828A-812A8815E3B4    7.5     https://vulners.com/githubexploit/E81474F6-6DDC-5FC2-828A-812A8815E3B4
E7B177F6-FA62-52FE-A108-4B8FC8112B7F    7.5     https://vulners.com/githubexploit/E7B177F6-FA62-52FE-A108-4B8FC8112B7F
E6B39247-8016-5007-B505-699F05FCA1B5    7.5     https://vulners.com/githubexploit/E6B39247-8016-5007-B505-699F05FCA1B5
E5C174E5-D6E8-56E0-8403-D287DE52EB3F    7.5     https://vulners.com/githubexploit/E5C174E5-D6E8-56E0-8403-D287DE52EB3F
E59A01BE-8176-5F5E-BD32-D30B009CDBDA    7.5     https://vulners.com/githubexploit/E59A01BE-8176-5F5E-BD32-D30B009CDBDA
E-739   7.5     https://vulners.com/dsquare/E-739       *EXPLOIT*
E-738   7.5     https://vulners.com/dsquare/E-738       *EXPLOIT*
DBF996C3-DC2A-5859-B767-6B2FC38F2185    7.5     https://vulners.com/githubexploit/DBF996C3-DC2A-5859-B767-6B2FC38F2185
DB6E1BBD-08B1-574D-A351-7D6BB9898A4A    7.5     https://vulners.com/githubexploit/DB6E1BBD-08B1-574D-A351-7D6BB9898A4A
D0E79214-C9E8-52BD-BC24-093970F5F34E    7.5     https://vulners.com/githubexploit/D0E79214-C9E8-52BD-BC24-093970F5F34E
CVE-2024-40898  7.5     https://vulners.com/cve/CVE-2024-40898
CVE-2024-39573  7.5     https://vulners.com/cve/CVE-2024-39573
CVE-2024-38477  7.5     https://vulners.com/cve/CVE-2024-38477
CVE-2024-38472  7.5     https://vulners.com/cve/CVE-2024-38472
CVE-2024-27316  7.5     https://vulners.com/cve/CVE-2024-27316
CVE-2023-43622  7.5     https://vulners.com/cve/CVE-2023-43622
CVE-2023-31122  7.5     https://vulners.com/cve/CVE-2023-31122
CVE-2023-27522  7.5     https://vulners.com/cve/CVE-2023-27522
CVE-2022-30556  7.5     https://vulners.com/cve/CVE-2022-30556
CVE-2022-30522  7.5     https://vulners.com/cve/CVE-2022-30522
CVE-2022-29404  7.5     https://vulners.com/cve/CVE-2022-29404
CVE-2022-26377  7.5     https://vulners.com/cve/CVE-2022-26377
CVE-2022-22719  7.5     https://vulners.com/cve/CVE-2022-22719
CVE-2021-41773  7.5     https://vulners.com/cve/CVE-2021-41773
CVE-2021-41524  7.5     https://vulners.com/cve/CVE-2021-41524
CVE-2021-36160  7.5     https://vulners.com/cve/CVE-2021-36160
```

```
CVE-2021-34798  7.5     https://vulners.com/cve/CVE-2021-34798
CVE-2021-31618  7.5     https://vulners.com/cve/CVE-2021-31618
CVE-2021-26690  7.5     https://vulners.com/cve/CVE-2021-26690
CVE-2020-13950  7.5     https://vulners.com/cve/CVE-2020-13950
CVE-2019-0215   7.5     https://vulners.com/cve/CVE-2019-0215
CVE-2019-0190   7.5     https://vulners.com/cve/CVE-2019-0190
CVE-2018-1303   7.5     https://vulners.com/cve/CVE-2018-1303
CVE-2017-9798   7.5     https://vulners.com/cve/CVE-2017-9798
CVE-2017-9789   7.5     https://vulners.com/cve/CVE-2017-9789
CVE-2017-7668   7.5     https://vulners.com/cve/CVE-2017-7668
CVE-2017-7659   7.5     https://vulners.com/cve/CVE-2017-7659
CVE-2017-15710  7.5     https://vulners.com/cve/CVE-2017-15710
CVE-2016-8743   7.5     https://vulners.com/cve/CVE-2016-8743
CVE-2009-2699   7.5     https://vulners.com/cve/CVE-2009-2699
CVE-2009-1955   7.5     https://vulners.com/cve/CVE-2009-1955
CVE-2006-20001  7.5     https://vulners.com/cve/CVE-2006-20001
CF47F8BF-37F7-5EF9-ABAB-E88ECF6B64FE    7.5     https://vulners.com/githubexploit/CF47F8BF-37F7-5EF9-ABAB-E88ECF6B64FE
CDC791CD-A414-5ABE-A897-7CFA3C2D3D29    7.5     https://vulners.com/githubexploit/CDC791CD-A414-5ABE-A897-7CFA3C2D3D29
CD48BD40-E52A-5A8B-AE27-B57C358BB0EE    7.5     https://vulners.com/githubexploit/CD48BD40-E52A-5A8B-AE27-B57C358BB0EE
C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B    7.5     https://vulners.com/githubexploit/C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B
C8C7BBD4-C089-5DA7-8474-A5B2B7DC5E79    7.5     https://vulners.com/githubexploit/C8C7BBD4-C089-5DA7-8474-A5B2B7DC5E79
C8799CA3-C88C-5B39-B291-2895BE0D9133    7.5     https://vulners.com/githubexploit/C8799CA3-C88C-5B39-B291-2895BE0D9133
C0380E16-C468-5540-A427-7FE34E7CF36B    7.5     https://vulners.com/githubexploit/C0380E16-C468-5540-A427-7FE34E7CF36B
BD3652A9-D066-57BA-9943-4E34970463B9    7.5     https://vulners.com/githubexploit/BD3652A9-D066-57BA-9943-4E34970463B9
BC027F41-02AD-5D71-A452-4DD62B0F1EE1    7.5     https://vulners.com/githubexploit/BC027F41-02AD-5D71-A452-4DD62B0F1EE1
B946B2A1-2914-537A-BF26-94B48FC501B3    7.5     https://vulners.com/githubexploit/B946B2A1-2914-537A-BF26-94B48FC501B3
B9151905-5395-5622-B789-E16B88F30C71    7.5     https://vulners.com/githubexploit/B9151905-5395-5622-B789-E16B88F30C71
B81BC21D-818E-5B33-96D7-062C14102874    7.5     https://vulners.com/githubexploit/B81BC21D-818E-5B33-96D7-062C14102874
B5E74010-A082-5ECE-AB37-623A5B33FE7D    7.5     https://vulners.com/githubexploit/B5E74010-A082-5ECE-AB37-623A5B33FE7D
B58E6202-6D04-5CB0-8529-59713C0E13B8    7.5     https://vulners.com/githubexploit/B58E6202-6D04-5CB0-8529-59713C0E13B8
B53D7077-1A2B-5640-9581-0196F6138301    7.5     https://vulners.com/githubexploit/B53D7077-1A2B-5640-9581-0196F6138301
B0208442-6E17-5772-B12D-B5BE30FA5540    7.5     https://vulners.com/githubexploit/B0208442-6E17-5772-B12D-B5BE30FA5540
A9C7FB0F-65EC-5557-B6E8-6AFBBF8F140F    7.5     https://vulners.com/githubexploit/A9C7FB0F-65EC-5557-B6E8-6AFBBF8F140F
A820A056-9F91-5059-B0BC-8D92C7A31A52    7.5     https://vulners.com/githubexploit/A820A056-9F91-5059-B0BC-8D92C7A31A52
A3F15BCE-08AD-509D-AE63-9D3D8E402E0B    7.5     https://vulners.com/githubexploit/A3F15BCE-08AD-509D-AE63-9D3D8E402E0B
A0F268C8-7319-5637-82F7-8DAF72D14629    7.5     https://vulners.com/githubexploit/A0F268C8-7319-5637-82F7-8DAF72D14629
9EE3F7E3-70E6-503E-9929-67FE3F3735A2    7.5     https://vulners.com/githubexploit/9EE3F7E3-70E6-503E-9929-67FE3F3735A2
9D511461-7D24-5402-8E2A-58364D6E758F    7.5     https://vulners.com/githubexploit/9D511461-7D24-5402-8E2A-58364D6E758F
9CEA663C-6236-5F45-B207-A873B971F988    7.5     https://vulners.com/githubexploit/9CEA663C-6236-5F45-B207-A873B971F988
987C6FDB-3E70-5FF5-AB5B-D50065D27594    7.5     https://vulners.com/githubexploit/987C6FDB-3E70-5FF5-AB5B-D50065D27594
9814661A-35A4-5DB7-BB25-A1040F365C81    7.5     https://vulners.com/githubexploit/9814661A-35A4-5DB7-BB25-A1040F365C81
89732403-A14E-5A5D-B659-DD4830410847    7.5     https://vulners.com/githubexploit/89732403-A14E-5A5D-B659-DD4830410847
7C40F14D-44E4-5155-95CF-40899776329C    7.5     https://vulners.com/githubexploit/7C40F14D-44E4-5155-95CF-40899776329C
789B6112-E84C-566E-89A7-82CC108EFCD9    7.5     https://vulners.com/githubexploit/789B6112-E84C-566E-89A7-82CC108EFCD9
788F7DF8-01F3-5D13-9B3E-E4AA692153E6    7.5     https://vulners.com/githubexploit/788F7DF8-01F3-5D13-9B3E-E4AA692153E6
749F952B-3ACF-56B2-809D-D66E756BE839    7.5     https://vulners.com/githubexploit/749F952B-3ACF-56B2-809D-D66E756BE839
6E484197-456B-55DF-8D51-C2BB4925F45C    7.5     https://vulners.com/githubexploit/6E484197-456B-55DF-8D51-C2BB4925F45C
6BCBA83C-4A4C-58D7-92E4-DF092DFEF267    7.5     https://vulners.com/githubexploit/6BCBA83C-4A4C-58D7-92E4-DF092DFEF267
68E78C64-D93A-5E8B-9DEA-4A8D826B474E    7.5     https://vulners.com/githubexploit/68E78C64-D93A-5E8B-9DEA-4A8D826B474E
68A13FF0-60E5-5A29-9248-83A940B0FB02    7.5     https://vulners.com/githubexploit/68A13FF0-60E5-5A29-9248-83A940B0FB02
6758CFA9-271A-5E99-A590-E51F4E0C5046    7.5     https://vulners.com/githubexploit/6758CFA9-271A-5E99-A590-E51F4E0C5046
674BA200-C494-57E6-B1B4-1672DDA15D3C    7.5     https://vulners.com/githubexploit/674BA200-C494-57E6-B1B4-1672DDA15D3C
5A864BCC-B490-5532-83AB-2E4109BB3C31    7.5     https://vulners.com/githubexploit/5A864BCC-B490-5532-83AB-2E4109BB3C31
5A54F5DA-F9C1-508B-AD2D-3E45CD647D31    7.5     https://vulners.com/githubexploit/5A54F5DA-F9C1-508B-AD2D-3E45CD647D31
4E5A5BA8-3BAF-57F0-B71A-F04B4D066E4F    7.5     https://vulners.com/githubexploit/4E5A5BA8-3BAF-57F0-B71A-F04B4D066E4F
4C79D8E5-D595-5460-AA84-18D4CB93E8FC    7.5     https://vulners.com/githubexploit/4C79D8E5-D595-5460-AA84-18D4CB93E8FC
45D138AD-BEC6-552A-91EA-8816914CA7F4    7.5     https://vulners.com/githubexploit/45D138AD-BEC6-552A-91EA-8816914CA7F4
41F0C2DA-2A2B-5ACC-A98D-CAD8D5AAD5ED    7.5     https://vulners.com/githubexploit/41F0C2DA-2A2B-5ACC-A98D-CAD8D5AAD5ED
4051D2EF-1C43-576D-ADB2-B519B31F93A0    7.5     https://vulners.com/githubexploit/4051D2EF-1C43-576D-ADB2-B519B31F93A0
3CF66144-235E-5F7A-B889-113C11ABF150    7.5     https://vulners.com/githubexploit/3CF66144-235E-5F7A-B889-113C11ABF150
379FCF38-0B4A-52EC-BE3E-408A0467BF20    7.5     https://vulners.com/githubexploit/379FCF38-0B4A-52EC-BE3E-408A0467BF20
365CD0B0-D956-59D6-9500-965BF4017E2D    7.5     https://vulners.com/githubexploit/365CD0B0-D956-59D6-9500-965BF4017E2D
2E98EA81-24D1-5D5B-80B9-A8D616BF3C3F    7.5     https://vulners.com/githubexploit/2E98EA81-24D1-5D5B-80B9-A8D616BF3C3F
2B4FEB27-377B-557B-AE46-66D677D5DA1C    7.5     https://vulners.com/githubexploit/2B4FEB27-377B-557B-AE46-66D677D5DA1C
2A177215-CE4A-5FA7-B016-EEAF332D165C    7.5     https://vulners.com/githubexploit/2A177215-CE4A-5FA7-B016-EEAF332D165C
1B75F2E2-5B30-58FA-98A4-501B91327D7F    7.5     https://vulners.com/githubexploit/1B75F2E2-5B30-58FA-98A4-501B91327D7F
18AE455A-1AA7-5386-81C2-39DA02CEFB57    7.5     https://vulners.com/githubexploit/18AE455A-1AA7-5386-81C2-39DA02CEFB57
17C6AD2A-8469-56C8-BBBE-1764D0DF1680    7.5     https://vulners.com/githubexploit/17C6AD2A-8469-56C8-BBBE-1764D0DF1680
1337DAY-ID-38427        7.5     https://vulners.com/zdt/1337DAY-ID-38427        *EXPLOIT*
1337DAY-ID-37030        7.5     https://vulners.com/zdt/1337DAY-ID-37030        *EXPLOIT*
1337DAY-ID-36937        7.5     https://vulners.com/zdt/1337DAY-ID-36937        *EXPLOIT*
1337DAY-ID-36897        7.5     https://vulners.com/zdt/1337DAY-ID-36897        *EXPLOIT*
1145F3D1-0ECB-55AA-B25D-A26892116505    7.5     https://vulners.com/githubexploit/1145F3D1-0ECB-55AA-B25D-A26892116505
108A0713-4AB8-5A1F-A16B-4BB13ECEC9B2    7.5     https://vulners.com/githubexploit/108A0713-4AB8-5A1F-A16B-4BB13ECEC9B2
0C28A0EC-7162-5D73-BEC9-B034F5392847    7.5     https://vulners.com/githubexploit/0C28A0EC-7162-5D73-BEC9-B034F5392847
0BC014D0-F944-5E78-B5FA-146A8E5D0F8A    7.5     https://vulners.com/githubexploit/0BC014D0-F944-5E78-B5FA-146A8E5D0F8A
06076ECD-3FB7-53EC-8572-ABBB20029812    7.5     https://vulners.com/githubexploit/06076ECD-3FB7-53EC-8572-ABBB20029812
05403438-4985-5E78-A702-784E03F724D4    7.5     https://vulners.com/githubexploit/05403438-4985-5E78-A702-784E03F724D4
00EC8F03-D8A3-56D4-9F8C-8DD1F5ACCA08    7.5     https://vulners.com/githubexploit/00EC8F03-D8A3-56D4-9F8C-8DD1F5ACCA08
CVE-2020-35452  7.3     https://vulners.com/cve/CVE-2020-35452
SSV:11802       7.1     https://vulners.com/seebug/SSV:11802    *EXPLOIT*
SSV:11762       7.1     https://vulners.com/seebug/SSV:11762    *EXPLOIT*
CVE-2009-1891   7.1     https://vulners.com/cve/CVE-2009-1891
CVE-2009-1890   7.1     https://vulners.com/cve/CVE-2009-1890
SSV:60427       6.9     https://vulners.com/seebug/SSV:60427    *EXPLOIT*
SSV:60386       6.9     https://vulners.com/seebug/SSV:60386    *EXPLOIT*
SSV:60069       6.9     https://vulners.com/seebug/SSV:60069    *EXPLOIT*
CVE-2012-0883   6.9     https://vulners.com/cve/CVE-2012-0883
SSV:12447       6.8     https://vulners.com/seebug/SSV:12447    *EXPLOIT*
PACKETSTORM:127546      6.8     https://vulners.com/packetstorm/PACKETSTORM:127546      *EXPLOIT*
FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8    6.8     https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8
CVE-2014-0226   6.8     https://vulners.com/cve/CVE-2014-0226
4427DEE4-E1E2-5A16-8683-D74750941604    6.8     https://vulners.com/githubexploit/4427DEE4-E1E2-5A16-8683-D74750941604
1337DAY-ID-22451        6.8     https://vulners.com/zdt/1337DAY-ID-22451        *EXPLOIT*
0095E929-7573-5E4A-A7FA-F6598A35E8DE    6.8     https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE
SSV:11568       6.4     https://vulners.com/seebug/SSV:11568    *EXPLOIT*
CVE-2009-1956   6.4     https://vulners.com/cve/CVE-2009-1956
CVE-2016-4975   6.1     https://vulners.com/cve/CVE-2016-4975
CVE-2023-45802  5.9     https://vulners.com/cve/CVE-2023-45802
CVE-2018-1302   5.9     https://vulners.com/cve/CVE-2018-1302
CVE-2018-1301   5.9     https://vulners.com/cve/CVE-2018-1301
VULNERLAB:967   5.8     https://vulners.com/vulnerlab/VULNERLAB:967     *EXPLOIT*
VULNERABLE:967  5.8     https://vulners.com/vulnerlab/VULNERABLE:967    *EXPLOIT*
SSV:67231       5.8     https://vulners.com/seebug/SSV:67231    *EXPLOIT*
SSV:18637       5.8     https://vulners.com/seebug/SSV:18637    *EXPLOIT*
```

```
SSV:15088       5.8     https://vulners.com/seebug/SSV:15088    *EXPLOIT*
SSV:12600       5.8     https://vulners.com/seebug/SSV:12600    *EXPLOIT*
PACKETSTORM:84112       5.8     https://vulners.com/packetstorm/PACKETSTORM:84112       *EXPLOIT*
EXPLOITPACK:8B4E7E8DAE5A13C8250C6C33307CD66C    5.8     https://vulners.com/exploitpack/EXPLOITPACK:8B4E7E8DAE5A13C8250
EDB-ID:10579    5.8     https://vulners.com/exploitdb/EDB-ID:10579      *EXPLOIT*
CVE-2009-3555   5.8     https://vulners.com/cve/CVE-2009-3555
45F0EB7B-CE04-5103-9D40-7379AE4B6CDD    5.8     https://vulners.com/githubexploit/45F0EB7B-CE04-5103-9D40-7379AE4B6CDD
CVE-2020-13938  5.5     https://vulners.com/cve/CVE-2020-13938
CVE-2024-40725  5.3     https://vulners.com/cve/CVE-2024-40725
CVE-2022-37436  5.3     https://vulners.com/cve/CVE-2022-37436
CVE-2022-28614  5.3     https://vulners.com/cve/CVE-2022-28614
CVE-2022-28330  5.3     https://vulners.com/cve/CVE-2022-28330
CVE-2021-30641  5.3     https://vulners.com/cve/CVE-2021-30641
CVE-2019-17567  5.3     https://vulners.com/cve/CVE-2019-17567
SSV:60788       5.1     https://vulners.com/seebug/SSV:60788    *EXPLOIT*
CVE-2013-1862   5.1     https://vulners.com/cve/CVE-2013-1862
SSV:96537       5.0     https://vulners.com/seebug/SSV:96537    *EXPLOIT*
SSV:62058       5.0     https://vulners.com/seebug/SSV:62058    *EXPLOIT*
SSV:61874       5.0     https://vulners.com/seebug/SSV:61874    *EXPLOIT*
SSV:20993       5.0     https://vulners.com/seebug/SSV:20993    *EXPLOIT*
SSV:20979       5.0     https://vulners.com/seebug/SSV:20979    *EXPLOIT*
SSV:20969       5.0     https://vulners.com/seebug/SSV:20969    *EXPLOIT*
SSV:19592       5.0     https://vulners.com/seebug/SSV:19592    *EXPLOIT*
SSV:15137       5.0     https://vulners.com/seebug/SSV:15137    *EXPLOIT*
SSV:12005       5.0     https://vulners.com/seebug/SSV:12005    *EXPLOIT*
PACKETSTORM:181059      5.0     https://vulners.com/packetstorm/PACKETSTORM:181059      *EXPLOIT*
PACKETSTORM:105672      5.0     https://vulners.com/packetstorm/PACKETSTORM:105672      *EXPLOIT*
PACKETSTORM:105591      5.0     https://vulners.com/packetstorm/PACKETSTORM:105591      *EXPLOIT*
MSF:AUXILIARY-SCANNER-HTTP-REWRITE_PROXY_BYPASS-        5.0     https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HT
EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D    5.0     https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C04
EXPLOITPACK:460143F0ACAE117DD79BD75EDFDA154B    5.0     https://vulners.com/exploitpack/EXPLOITPACK:460143F0ACAE117DD79
EDB-ID:17969    5.0     https://vulners.com/exploitdb/EDB-ID:17969      *EXPLOIT*
CVE-2015-3183   5.0     https://vulners.com/cve/CVE-2015-3183
CVE-2015-0228   5.0     https://vulners.com/cve/CVE-2015-0228
CVE-2014-0231   5.0     https://vulners.com/cve/CVE-2014-0231
CVE-2014-0098   5.0     https://vulners.com/cve/CVE-2014-0098
CVE-2013-6438   5.0     https://vulners.com/cve/CVE-2013-6438
CVE-2013-5704   5.0     https://vulners.com/cve/CVE-2013-5704
CVE-2011-3368   5.0     https://vulners.com/cve/CVE-2011-3368
CVE-2010-1623   5.0     https://vulners.com/cve/CVE-2010-1623
CVE-2010-1452   5.0     https://vulners.com/cve/CVE-2010-1452
CVE-2010-0408   5.0     https://vulners.com/cve/CVE-2010-0408
CVE-2009-3720   5.0     https://vulners.com/cve/CVE-2009-3720
CVE-2009-3560   5.0     https://vulners.com/cve/CVE-2009-3560
CVE-2009-3095   5.0     https://vulners.com/cve/CVE-2009-3095
CVE-2008-2364   5.0     https://vulners.com/cve/CVE-2008-2364
CVE-2007-6750   5.0     https://vulners.com/cve/CVE-2007-6750
1337DAY-ID-28573        5.0     https://vulners.com/zdt/1337DAY-ID-28573        *EXPLOIT*
SSV:11668       4.9     https://vulners.com/seebug/SSV:11668    *EXPLOIT*
SSV:11501       4.9     https://vulners.com/seebug/SSV:11501    *EXPLOIT*
CVE-2009-1195   4.9     https://vulners.com/cve/CVE-2009-1195
SSV:30024       4.6     https://vulners.com/seebug/SSV:30024    *EXPLOIT*
CVE-2012-0031   4.6     https://vulners.com/cve/CVE-2012-0031
1337DAY-ID-27465        4.6     https://vulners.com/zdt/1337DAY-ID-27465        *EXPLOIT*
SSV:23169       4.4     https://vulners.com/seebug/SSV:23169    *EXPLOIT*
CVE-2011-3607   4.4     https://vulners.com/cve/CVE-2011-3607
1337DAY-ID-27473        4.4     https://vulners.com/zdt/1337DAY-ID-27473        *EXPLOIT*
SSV:60905       4.3     https://vulners.com/seebug/SSV:60905    *EXPLOIT*
SSV:60657       4.3     https://vulners.com/seebug/SSV:60657    *EXPLOIT*
SSV:60653       4.3     https://vulners.com/seebug/SSV:60653    *EXPLOIT*
SSV:60345       4.3     https://vulners.com/seebug/SSV:60345    *EXPLOIT*
SSV:4786        4.3     https://vulners.com/seebug/SSV:4786     *EXPLOIT*
SSV:3804        4.3     https://vulners.com/seebug/SSV:3804     *EXPLOIT*
SSV:30094       4.3     https://vulners.com/seebug/SSV:30094    *EXPLOIT*
SSV:30056       4.3     https://vulners.com/seebug/SSV:30056    *EXPLOIT*
SSV:24250       4.3     https://vulners.com/seebug/SSV:24250    *EXPLOIT*
SSV:20555       4.3     https://vulners.com/seebug/SSV:20555    *EXPLOIT*
SSV:19320       4.3     https://vulners.com/seebug/SSV:19320    *EXPLOIT*
SSV:11558       4.3     https://vulners.com/seebug/SSV:11558    *EXPLOIT*
PACKETSTORM:109284      4.3     https://vulners.com/packetstorm/PACKETSTORM:109284      *EXPLOIT*
FFE89CAE-FAA6-5E93-9994-B5F4D0EC2197    4.3     https://vulners.com/githubexploit/FFE89CAE-FAA6-5E93-9994-B5F4D0EC2197
F893E602-F8EB-5D23-8ABF-920890DB23A3    4.3     https://vulners.com/githubexploit/F893E602-F8EB-5D23-8ABF-920890DB23A3
F463914D-1B20-54CA-BF87-EA28F3ADE2A3    4.3     https://vulners.com/githubexploit/F463914D-1B20-54CA-BF87-EA28F3ADE2A3
EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE    4.3     https://vulners.com/exploitpack/EXPLOITPACK:FDCB3D93694E48CD5EE
EDB-ID:35738    4.3     https://vulners.com/exploitdb/EDB-ID:35738      *EXPLOIT*
ECD5D758-774C-5488-B782-C8996208B401    4.3     https://vulners.com/githubexploit/ECD5D758-774C-5488-B782-C8996208B401
E9FE319B-26BF-5A75-8C6A-8AE55D7E7615    4.3     https://vulners.com/githubexploit/E9FE319B-26BF-5A75-8C6A-8AE55D7E7615
DF57E8F1-FE21-5EB9-8FC7-5F2EA267B09D    4.3     https://vulners.com/githubexploit/DF57E8F1-FE21-5EB9-8FC7-5F2EA267B09D
D7922C26-D431-5825-9897-B98478354289    4.3     https://vulners.com/githubexploit/D7922C26-D431-5825-9897-B98478354289
CVE-2016-8612   4.3     https://vulners.com/cve/CVE-2016-8612
CVE-2014-0118   4.3     https://vulners.com/cve/CVE-2014-0118
CVE-2013-1896   4.3     https://vulners.com/cve/CVE-2013-1896
CVE-2012-4558   4.3     https://vulners.com/cve/CVE-2012-4558
CVE-2012-3499   4.3     https://vulners.com/cve/CVE-2012-3499
CVE-2012-0053   4.3     https://vulners.com/cve/CVE-2012-0053
CVE-2011-4317   4.3     https://vulners.com/cve/CVE-2011-4317
CVE-2011-3639   4.3     https://vulners.com/cve/CVE-2011-3639
CVE-2011-0419   4.3     https://vulners.com/cve/CVE-2011-0419
CVE-2010-0434   4.3     https://vulners.com/cve/CVE-2010-0434
CVE-2009-0023   4.3     https://vulners.com/cve/CVE-2009-0023
CVE-2008-2939   4.3     https://vulners.com/cve/CVE-2008-2939
CVE-2008-0455   4.3     https://vulners.com/cve/CVE-2008-0455
CVE-2007-6420   4.3     https://vulners.com/cve/CVE-2007-6420
C26A395B-9695-59E4-908F-866A561936E9    4.3     https://vulners.com/githubexploit/C26A395B-9695-59E4-908F-866A561936E9
C068A003-5258-51DC-A3C0-786638A1B69C    4.3     https://vulners.com/githubexploit/C068A003-5258-51DC-A3C0-786638A1B69C
B8198D62-F9C8-5E03-A301-9A3580070B4C    4.3     https://vulners.com/githubexploit/B8198D62-F9C8-5E03-A301-9A3580070B4C
B4483895-BA86-5CFB-84F3-7C06411B5175    4.3     https://vulners.com/githubexploit/B4483895-BA86-5CFB-84F3-7C06411B5175
A6753173-D2DC-54CC-A5C4-0751E61F0343    4.3     https://vulners.com/githubexploit/A6753173-D2DC-54CC-A5C4-0751E61F0343
A1FF76C0-CF98-5704-AEE4-DF6F1E434FA3    4.3     https://vulners.com/githubexploit/A1FF76C0-CF98-5704-AEE4-DF6F1E434FA3
8FB9E7A8-9A5B-5D87-9A44-AE4A1A92213D    4.3     https://vulners.com/githubexploit/8FB9E7A8-9A5B-5D87-9A44-AE4A1A92213D
8A14FEAD-A401-5B54-84EB-2059841AD1DD    4.3     https://vulners.com/githubexploit/8A14FEAD-A401-5B54-84EB-2059841AD1DD
7248BA4C-3FE5-5529-9E4C-C91E241E8AA0    4.3     https://vulners.com/githubexploit/7248BA4C-3FE5-5529-9E4C-C91E241E8AA0
6E104766-2F7A-5A0A-A24B-61D9B52AD4EE    4.3     https://vulners.com/githubexploit/6E104766-2F7A-5A0A-A24B-61D9B52AD4EE
6C0C909F-3307-5755-97D2-0EBD17367154    4.3     https://vulners.com/githubexploit/6C0C909F-3307-5755-97D2-0EBD17367154
628A345B-5FD8-5A2F-8782-9125584E4C89    4.3     https://vulners.com/githubexploit/628A345B-5FD8-5A2F-8782-9125584E4C89
```

```
        5D88E443-7AB2-5034-910D-D52A5EFFF5FC    4.3     https://vulners.com/githubexploit/5D88E443-7AB2-5034-910D-D52A5EFFF5FC
        500CE683-17EB-5776-8EF6-85122451B145    4.3     https://vulners.com/githubexploit/500CE683-17EB-5776-8EF6-85122451B145
        4E4BAF15-6430-514A-8679-5B9F03584B71    4.3     https://vulners.com/githubexploit/4E4BAF15-6430-514A-8679-5B9F03584B71
        4B46EB21-DF1F-5D84-AE44-9BCFE311DFB9    4.3     https://vulners.com/githubexploit/4B46EB21-DF1F-5D84-AE44-9BCFE311DFB9
        4B44115D-85A3-5E62-B9A8-5F336C24673F    4.3     https://vulners.com/githubexploit/4B44115D-85A3-5E62-B9A8-5F336C24673F
        3C5B500C-1858-5834-9D23-38DBE44AE969    4.3     https://vulners.com/githubexploit/3C5B500C-1858-5834-9D23-38DBE44AE969
        3B159471-590A-5941-ADED-20F4187E8C63    4.3     https://vulners.com/githubexploit/3B159471-590A-5941-ADED-20F4187E8C63
        3AE03E90-26EC-5F91-B84E-F04AF6239A9F    4.3     https://vulners.com/githubexploit/3AE03E90-26EC-5F91-B84E-F04AF6239A9F
        37A9128D-17C4-50FF-B025-5FC3E0F3F338    4.3     https://vulners.com/githubexploit/37A9128D-17C4-50FF-B025-5FC3E0F3F338
        3749CB78-BE3A-5018-8838-CA693845B5BD    4.3     https://vulners.com/githubexploit/3749CB78-BE3A-5018-8838-CA693845B5BD
        27108E72-8DC1-53B5-97D9-E869CA13EFF7    4.3     https://vulners.com/githubexploit/27108E72-8DC1-53B5-97D9-E869CA13EFF7
        24ADD37D-C8A1-5671-A0F4-378760FC69AC    4.3     https://vulners.com/githubexploit/24ADD37D-C8A1-5671-A0F4-378760FC69AC
        1E6E9010-4BDF-5C30-951C-79C280B90883    4.3     https://vulners.com/githubexploit/1E6E9010-4BDF-5C30-951C-79C280B90883
        1337DAY-ID-36854        4.3     https://vulners.com/zdt/1337DAY-ID-36854        *EXPLOIT*
        04E3583E-DFED-5D0D-BCF2-1C1230EB666D    4.3     https://vulners.com/githubexploit/04E3583E-DFED-5D0D-BCF2-1C1230EB666D
        SSV:12628       2.6     https://vulners.com/seebug/SSV:12628    *EXPLOIT*
        CVE-2012-2687   2.6     https://vulners.com/cve/CVE-2012-2687
        CVE-2009-3094   2.6     https://vulners.com/cve/CVE-2009-3094
        CVE-2008-0456   2.6     https://vulners.com/cve/CVE-2008-0456
        SSV:60250       1.2     https://vulners.com/seebug/SSV:60250    *EXPLOIT*
        CVE-2011-4415   1.2     https://vulners.com/cve/CVE-2011-4415
        PACKETSTORM:164501      0.0     https://vulners.com/packetstorm/PACKETSTORM:164501      *EXPLOIT*
        PACKETSTORM:164418      0.0     https://vulners.com/packetstorm/PACKETSTORM:164418      *EXPLOIT*
        EDB-ID:8842     0.0     https://vulners.com/exploitdb/EDB-ID:8842       *EXPLOIT*
        EDB-ID:41769    0.0     https://vulners.com/exploitdb/EDB-ID:41769      *EXPLOIT*
        EDB-ID:41768    0.0     https://vulners.com/exploitdb/EDB-ID:41768      *EXPLOIT*
        EDB-ID:36663    0.0     https://vulners.com/exploitdb/EDB-ID:36663      *EXPLOIT*
        EDB-ID:36352    0.0     https://vulners.com/exploitdb/EDB-ID:36352      *EXPLOIT*
        EDB-ID:34133    0.0     https://vulners.com/exploitdb/EDB-ID:34133      *EXPLOIT*
        EDB-ID:31052    0.0     https://vulners.com/exploitdb/EDB-ID:31052      *EXPLOIT*
        EDB-ID:18442    0.0     https://vulners.com/exploitdb/EDB-ID:18442      *EXPLOIT*
        EDB-ID:17696    0.0     https://vulners.com/exploitdb/EDB-ID:17696      *EXPLOIT*
        EDB-ID:10071    0.0     https://vulners.com/exploitdb/EDB-ID:10071      *EXPLOIT*
        CVE-2024-39884  0.0     https://vulners.com/cve/CVE-2024-39884
        CVE-2024-36387  0.0     https://vulners.com/cve/CVE-2024-36387
        CVE-2024-24795  0.0     https://vulners.com/cve/CVE-2024-24795
        CVE-2023-38709  0.0     https://vulners.com/cve/CVE-2023-38709
        1337DAY-ID-9602 0.0     https://vulners.com/zdt/1337DAY-ID-9602 *EXPLOIT*
        1337DAY-ID-21346        0.0     https://vulners.com/zdt/1337DAY-ID-21346        *EXPLOIT*
        1337DAY-ID-17257        0.0     https://vulners.com/zdt/1337DAY-ID-17257        *EXPLOIT*
        1337DAY-ID-16843        0.0     https://vulners.com/zdt/1337DAY-ID-16843        *EXPLOIT*
        1337DAY-ID-13268        0.0     https://vulners.com/zdt/1337DAY-ID-13268        *EXPLOIT*
        1337DAY-ID-11185        0.0     https://vulners.com/zdt/1337DAY-ID-11185        *EXPLOIT*
```

http-csrf

```
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.50.100
  Found the following possible CSRF vulnerabilities:

    Path: http://192.168.50.100:80/dvwa/
    Form id:
    Form action: login.php

    Path: http://192.168.50.100:80/mutillidae/?page=source-viewer.php
    Form id: id-bad-cred-tr
    Form action: index.php?page=source-viewer.php

    Path: http://192.168.50.100:80/mutillidae/index.php?page=user-poll.php
    Form id: idpollform
    Form action: index.php

    Path: http://192.168.50.100:80/mutillidae/?page=text-file-viewer.php
    Form id: id-bad-cred-tr
    Form action: index.php?page=text-file-viewer.php

    Path: http://192.168.50.100:80/mutillidae/index.php?page=user-info.php
    Form id: id-bad-cred-tr
    Form action: ./index.php?page=user-info.php
```

http-brute

```
  Path "/" does not require authentication
```

http-sitemap-generator

```
  Directory structure:
    /
      Other: 1
    /dav/
      Other: 1
    /dvwa/
      Other: 1
    /icons/
      gif: 2
    /mutillidae/
      Other: 1; php: 2
    /mutillidae/images/
      jpg: 1
    /mutillidae/styles/ddsmoothmenu/
      css: 1
    /phpMyAdmin/
      Other: 1
    /twiki/
      Other: 1
  Longest directory structure:
    Depth: 3
    Dir: /mutillidae/styles/ddsmoothmenu/
  Total files found (by extension):
    Other: 6; css: 1; gif: 2; jpg: 1; php: 2
```

http-useragent-tester

```
  Status for browser useragent: 200
  Allowed User Agents:
    Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
    libwww
    lwp-trivial
    libcurl-agent/1.0
    PHP/
    Python-urllib/2.5
    GT::WWW
    Snoopy
    MFC_Tear_Sample
    HTTP::Lite
    PHPCrawl
    URI::Fetch
    Zend_Http_Client
    http client
    PECL::HTTP
    Wget/1.13.4 (linux-gnu)
    WWW-Mechanize/1.34
```

http-dombased-xss

```
Couldn't find any DOM based XSS.
```

http-title

```
Metasploitable2 - Linux
```

http-date

```
Fri, 27 Sep 2024 19:48:46 GMT; -2s from local time.
```

http-chrono

```
Request times for /; avg: 261.32ms; min: 210.31ms; max: 447.89ms
```

http-mobileversion-checker

```
No mobile version detected.
```

http-server-header

```
Apache/2.2.8 (Ubuntu) DAV/2
```

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-sql-injection

```
  Possible sqli for queries:
    http://192.168.50.100:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
    http://192.168.50.100:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
    http://192.168.50.100:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
    http://192.168.50.100:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27
    http://192.168.50.100:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/?page=login.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
    http://192.168.50.100:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
    http://192.168.50.100:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
    http://192.168.50.100:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
    http://192.168.50.100:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
    http://192.168.50.100:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
    http://192.168.50.100:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
    http://192.168.50.100:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
    http://192.168.50.100:80/dav/?C=M%3BO%3DD%27%20OR%20sqlspider
    http://192.168.50.100:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
    http://192.168.50.100:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
```

```
http://192.168.50.100:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
http://192.168.50.100:80/dav/?C=D%3BO%3DD%27%20OR%20sqlspider
http://192.168.50.100:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
http://192.168.50.100:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
http://192.168.50.100:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
http://192.168.50.100:80/dav/?C=S%3BO%3DD%27%20OR%20sqlspider
http://192.168.50.100:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
http://192.168.50.100:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27
http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
http://192.168.50.100:80/mutillidae/?page=login.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27
http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=login.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
http://192.168.50.100:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27
http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
```

```
http://192.168.50.100:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
http://192.168.50.100:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=login.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27
http://192.168.50.100:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
http://192.168.50.100:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=login.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27
http://192.168.50.100:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
http://192.168.50.100:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=login.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.issa-
http://192.168.50.100:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.owasp
http://192.168.50.100:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.pocod
http://192.168.50.100:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.php.n
http://192.168.50.100:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.isd-p
http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.room3
http://192.168.50.100:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.owasp
http://192.168.50.100:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27
```

```
  http://192.168.50.100:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=https%3A%2F%2Faddons.m
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fpauldotco
  http://192.168.50.100:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.irong
  http://192.168.50.100:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=login.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
  http://192.168.50.100:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.issa-
  http://192.168.50.100:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.owasp
  http://192.168.50.100:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.pocod
  http://192.168.50.100:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.php.n
  http://192.168.50.100:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.isd-p
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.room3
  http://192.168.50.100:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.owasp
  http://192.168.50.100:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27
  http://192.168.50.100:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=https%3A%2F%2Faddons.m
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fpauldotco
  http://192.168.50.100:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=redirectandlog.php%27%20OR%20sqlspider&forwardurl=http%3A%2F%2Fwww.irong
  http://192.168.50.100:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=login.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
  http://192.168.50.100:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=register.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27
  http://192.168.50.100:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
  http://192.168.50.100:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/?page=login.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
  http://192.168.50.100:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
Possible sqli for forms:
  Form at path: /mutillidae/index.php, form's action: index.php. Fields that might be vulnerable:
    choice
    choice
    choice
    choice
    choice
    choice
    choice
    choice
    choice
    choice
    choice
    choice
    initials
  Form at path: /mutillidae/index.php, form's action: ./index.php?page=user-info.php. Fields that might be vulnerable:
    username
```

http-unsafe-output-escaping

```
  Characters [> " '] reflected in parameter page at http://192.168.50.100:80/mutillidae/?page=source-viewer.php
  Characters [> " '] reflected in parameter page at http://192.168.50.100:80/mutillidae/index.php?page=user-poll.php
  Characters [> " '] reflected in parameter page at http://192.168.50.100:80/mutillidae/index.php?page=notes.php
  Characters [> " '] reflected in parameter page at http://192.168.50.100:80/mutillidae/?page=text-file-viewer.php
  Characters [> " '] reflected in parameter page at http://192.168.50.100:80/mutillidae/index.php?page=arbitrary-file-inclusion
  Characters [> " '] reflected in parameter page at http://192.168.50.100:80/mutillidae/?page=credits.php
  Characters [> " '] reflected in parameter page at http://192.168.50.100:80/mutillidae/index.php?page=credits.php
  Characters [> " '] reflected in parameter page at http://192.168.50.100:80/mutillidae/index.php?page=user-info.php
```

http-devframework

```
Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.
```

http-stored-xss

```
Couldn't find any stored XSS vulnerabilities.
```

http-auth-finder

```
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.50.100
  url                                                              method
  http://192.168.50.100:80/phpMyAdmin/                             FORM
  http://192.168.50.100:80/dvwa/                                   FORM
  http://192.168.50.100:80/mutillidae/index.php?page=user-info.php  FORM
```

http-referer-checker

```
Couldn't find any cross-domain scripts.
```

http-comments-displayer

```
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.50.100

    Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
    Line number: 81
    Comment:
        /*Holly Hack for IE7 and below*/

    Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
    Line number: 98
    Comment:
        /* ######### CSS for shadow added to sub menus  ######### */

    Path: http://192.168.50.100:80/phpMyAdmin/
    Line number: 66
    Comment:

        // <![CDATA[

    Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
    Line number: 55
    Comment:
        /*collapse all sub menus to begin with*/

    Path: http://192.168.50.100:80/mutillidae/index.php?page=user-info.php
    Line number: 32
    Comment:


    Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
    Line number: 51
    Comment:
        /*1st sub level menu*/

    Path: http://192.168.50.100:80/phpMyAdmin/
    Line number: 44
    Comment:
        <!-- Login form -->

    Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
    Line number: 73
    Comment:
        /*width of sub menus*/

    Path: http://192.168.50.100:80/dvwa/
    Line number: 61
    Comment:
        <!-- end align div -->

    Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
    Line number: 41
    Comment:
        /*CSS class that's dynamically added to the currently active menu items' LI A element*/

    Path: http://192.168.50.100:80/mutillidae/index.php?page=user-info.php
    Line number: 488
    Comment:
        <!-- Begin Content -->

    Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
    Line number: 14
    Comment:
        /*Top level list items*/
Path: http://192.168.50.100:80/mutillidae/index.php?page=user-info.php
Line number: 31
Comment:


Path: http://192.168.50.100:80/mutillidae/index.php?page=user-info.php
Line number: 23
Comment:




                    ***********************************************/

Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
Line number: 70
Comment:
    /* Sub level menu links style */

Path: http://192.168.50.100:80/phpMyAdmin/
Line number: 18
Comment:

    //]]>

Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
Line number: 84
Comment:
    /* ######### CSS classes applied to down and right arrow images  ######### */

Path: http://192.168.50.100:80/phpMyAdmin/
Line number: 13
Comment:

    //<![CDATA[

Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
Line number: 59
Comment:
    /*Sub level menu list items (undo style from Top level List Items)*/

Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
Line number: 100
Comment:
    /*shadow for NON CSS3 capable browsers*/

Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
Line number: 109
Comment:
    /*shadow opacity for NON CSS3 capable browsers. Doesn't work in IE*/

Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
Line number: 65
Comment:
    /*All subsequent sub menu levels vertical offset after 1st level sub menu */

Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
Line number: 24
Comment:
    /*background of menu items (default state)*/

Path: http://192.168.50.100:80/mutillidae/index.php?page=user-info.php
Line number: 35
Comment:


Path: http://192.168.50.100:80/mutillidae/index.php?page=user-info.php
Line number: 2
Comment:






                            security instructors are just making all this up. -->

Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
Line number: 47
Comment:
    /*background of menu items during onmouseover (hover state)*/

Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
Line number: 3
Comment:
    /*background of menu bar (default state)*/

Path: http://192.168.50.100:80/mutillidae/index.php?page=user-info.php
Line number: 547
Comment:
    <!-- End Content -->

Path: http://192.168.50.100:80/mutillidae/index.php?page=user-info.php
Line number: 33
Comment:


Path: http://192.168.50.100:80/phpMyAdmin/
Line number: 79
Comment:

    // ]]>

Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
```

```
  Line number: 21
  Comment:
      /*Top level menu link items style*/

  Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
  Line number: 33
  Comment:
      /*IE6 hack to get sub menu links to behave correctly*/

  Path: http://192.168.50.100:80/dvwa/
  Line number: 57
  Comment:
      <!-- <img src="dvwa/images/RandomStorm.png" /> -->

  Path: http://192.168.50.100:80/mutillidae/styles/ddsmoothmenu/ddsmoothmenu.css
  Line number: 80
  Comment:
      /* Holly Hack for IE \*/
```

111	tcp	open	rpcbind	syn-ac

nfs-ls

```
Volume /
  access: Read Lookup Modify Extend Delete NoExecute
PERMISSION  UID  GID  SIZE   TIME                 FILENAME
-rw-r--r--  0    0    0      2024-09-23T18:00:51  GBTJL\x03}
drwxr-xr-x  0    0    4096   2012-05-14T03:35:33  bin
drwxr-xr-x  0    0    4096   2010-04-16T06:16:02  home
drwxr-xr-x  0    0    4096   2010-03-16T22:57:40  initrd
lrwxrwxrwx  0    0    32     2010-04-28T20:26:18  initrd.img
drwxr-xr-x  0    0    4096   2012-05-14T03:35:22  lib
drwx------  0    0    16384  2010-03-16T22:55:15  lost+found
drwxr-xr-x  0    0    4096   2010-03-16T22:55:52  media
drwxr-xr-x  0    0    4096   2010-04-28T20:16:56  mnt
drwxr-xr-x  0    0    4096   2012-05-14T01:54:53  sbin
```

nfs-showmount

```
  / *
```

nfs-statfs

```
  Filesystem  1K-blocks  Used       Available  Use%  Maxfilesize  Maxlink
  /           7282168.0  1500192.0  5414976.0  22%   2.0T         32000
```

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      34181/tcp   mountd
  100005  1,2,3      50953/udp   mountd
  100021  1,3,4      34002/udp   nlockmgr
  100021  1,3,4      40607/tcp   nlockmgr
  100024  1          47589/tcp   status
  100024  1          60598/udp   status
```

139	tcp	open	netbios-ssn	syn-ac
445	tcp	open	netbios-ssn	syn-ac
512	tcp	open	exec	syn-ac

rexec-brute

```
  Accounts: No valid accounts found
  Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
  ERROR: The service seems to have failed or is heavily firewalled...
```

banner

```
\x01Where are you?
```

513	tcp	open	login	syn-ac

rlogin-brute

```
  Accounts: No valid accounts found
  Statistics: Performed 18 guesses in 3647 seconds, average tps: 0.0
```

514	tcp	open	shell	syn-ac

banner

```
\x01getnameinfo: Temporary failure in name resolution
```

1099	tcp	open	java-rmi	syn-ac

unusual-port

```
java-rmi unexpected on port tcp/1099
```

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	bindshell	syn-ac

banner

```
root@metasploitable:/#
```

unusual-port

```
bindshell unexpected on port tcp/1524
```

2049	tcp	open	nfs	syn-ac

unusual-port

```
rpcbind unexpected on port tcp/2049
```

2121	tcp	open	ccproxy-ftp	syn-ac
3306	tcp	open	mysql	syn-ac

banner

```
>\x00\x00\x00\x0A5.0.51a-3ubuntu5\x00\x0D\x00\x00\x00X]LCK1Q...
```

mysql-enum

```
  Accounts: No valid accounts found
  Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
  ERROR: The service seems to have failed or is heavily firewalled...
```

vulners

```
  cpe:/a:mysql:mysql:5.0.51a-3ubuntu5:
        SSV:15006       6.8     https://vulners.com/seebug/SSV:15006    *EXPLOIT*
        CVE-2009-4028   6.8     https://vulners.com/cve/CVE-2009-4028
        SSV:3280        4.6     https://vulners.com/seebug/SSV:3280     *EXPLOIT*
        CVE-2008-2079   4.6     https://vulners.com/cve/CVE-2008-2079
        CVE-2010-3682   4.0     https://vulners.com/cve/CVE-2010-3682
        CVE-2010-3677   4.0     https://vulners.com/cve/CVE-2010-3677
        EDB-ID:34506    0.0     https://vulners.com/exploitdb/EDB-ID:34506      *EXPLOIT*
```

mysql-brute

```
  Accounts: No valid accounts found
  Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
  ERROR: The service seems to have failed or is heavily firewalled...
```

mysql-info

```
  Protocol: 10
  Version: 5.0.51a-3ubuntu5
  Thread ID: 11
  Capabilities flags: 43564
  Some Capabilities: Speaks41ProtocolNew, ConnectWithDatabase, Support41Auth, LongColumnFlag, SupportsTransactions, SwitchToSSL
  Status: Autocommit
  Salt: Y5:djiM'u?tOnZY.w2.1
```

3632	tcp	open	distccd	syn-ac

distcc-cve2004-2687

```
  VULNERABLE:
  distcc Daemon Command Execution
    State: VULNERABLE (Exploitable)
    IDs:  CVE:CVE-2004-2687
    Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
      Allows executing of arbitrary commands on systems running distccd 3.1 and
      earlier. The vulnerability is the consequence of weak service configuration.

    Disclosure date: 2002-02-01
    Extra information:

    uid=1(daemon) gid=1(daemon) groups=1(daemon)

    References:
      https://nvd.nist.gov/vuln/detail/CVE-2004-2687
      https://distcc.github.io/security.html
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
```

5432	tcp	open	postgresql	syn-ac

ssl-cert

```
Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/cou
Not valid before: 2010-03-17T14:07:45
Not valid after:  2010-04-16T14:07:45
```

vulners

```
  cpe:/a:postgresql:postgresql:8.3:
        SSV:60718       10.0    https://vulners.com/seebug/SSV:60718    *EXPLOIT*
        CVE-2013-1903   10.0    https://vulners.com/cve/CVE-2013-1903
        CVE-2013-1902   10.0    https://vulners.com/cve/CVE-2013-1902
        CVE-2019-10211  9.8     https://vulners.com/cve/CVE-2019-10211
        CVE-2015-3166   9.8     https://vulners.com/cve/CVE-2015-3166
        CVE-2015-0244   9.8     https://vulners.com/cve/CVE-2015-0244
        CVE-2018-1115   9.1     https://vulners.com/cve/CVE-2018-1115
        CVE-2022-1552   8.8     https://vulners.com/cve/CVE-2022-1552
        CVE-2021-32027  8.8     https://vulners.com/cve/CVE-2021-32027
        CVE-2020-25695  8.8     https://vulners.com/cve/CVE-2020-25695
        CVE-2019-10164  8.8     https://vulners.com/cve/CVE-2019-10164
        CVE-2019-10127  8.8     https://vulners.com/cve/CVE-2019-10127
        CVE-2015-0243   8.8     https://vulners.com/cve/CVE-2015-0243
        CVE-2015-0242   8.8     https://vulners.com/cve/CVE-2015-0242
        CVE-2015-0241   8.8     https://vulners.com/cve/CVE-2015-0241
        SSV:30015       8.5     https://vulners.com/seebug/SSV:30015    *EXPLOIT*
        SSV:19652       8.5     https://vulners.com/seebug/SSV:19652    *EXPLOIT*
        CVE-2010-1447   8.5     https://vulners.com/cve/CVE-2010-1447
        CVE-2010-1169   8.5     https://vulners.com/cve/CVE-2010-1169
        CVE-2016-5423   8.3     https://vulners.com/cve/CVE-2016-5423
        CVE-2021-23214  8.1     https://vulners.com/cve/CVE-2021-23214
        CVE-2020-25694  8.1     https://vulners.com/cve/CVE-2020-25694
        CVE-2016-7048   8.1     https://vulners.com/cve/CVE-2016-7048
        CVE-2022-2625   8.0     https://vulners.com/cve/CVE-2022-2625
        CVE-2019-10128  7.8     https://vulners.com/cve/CVE-2019-10128
        SSV:19754       7.5     https://vulners.com/seebug/SSV:19754    *EXPLOIT*
        CVE-2020-25696  7.5     https://vulners.com/cve/CVE-2020-25696
        CVE-2017-7484   7.5     https://vulners.com/cve/CVE-2017-7484
        CVE-2016-0773   7.5     https://vulners.com/cve/CVE-2016-0773
        CVE-2016-0768   7.5     https://vulners.com/cve/CVE-2016-0768
        CVE-2015-3167   7.5     https://vulners.com/cve/CVE-2015-3167
        EDB-ID:45184    7.3     https://vulners.com/exploitdb/EDB-ID:45184      *EXPLOIT*
        CVE-2020-14350  7.3     https://vulners.com/cve/CVE-2020-14350
        CVE-2020-10733  7.3     https://vulners.com/cve/CVE-2020-10733
        CVE-2017-14798  7.3     https://vulners.com/cve/CVE-2017-14798
```

```
    CVE-2023-2454   7.2     https://vulners.com/cve/CVE-2023-2454
    CVE-2020-14349  7.1     https://vulners.com/cve/CVE-2020-14349
    CVE-2016-5424   7.1     https://vulners.com/cve/CVE-2016-5424
    CVE-2019-10210  7.0     https://vulners.com/cve/CVE-2019-10210
    PACKETSTORM:148884      6.9     https://vulners.com/packetstorm/PACKETSTORM:148884      *EXPLOIT*
    EXPLOITPACK:6F8D33BC4F1C65AE0911D23B5E6EB665    6.9     https://vulners.com/exploitpack/EXPLOITPACK:6F8D33BC4F1C65AE091
    1337DAY-ID-30875        6.9     https://vulners.com/zdt/1337DAY-ID-30875        *EXPLOIT*
    SSV:30152       6.8     https://vulners.com/seebug/SSV:30152    *EXPLOIT*
    CVE-2013-0255   6.8     https://vulners.com/cve/CVE-2013-0255
    CVE-2012-0868   6.8     https://vulners.com/cve/CVE-2012-0868
    CVE-2009-3231   6.8     https://vulners.com/cve/CVE-2009-3231
    SSV:62083       6.5     https://vulners.com/seebug/SSV:62083    *EXPLOIT*
    SSV:62016       6.5     https://vulners.com/seebug/SSV:62016    *EXPLOIT*
    SSV:61543       6.5     https://vulners.com/seebug/SSV:61543    *EXPLOIT*
    SSV:19018       6.5     https://vulners.com/seebug/SSV:19018    *EXPLOIT*
    CVE-2021-3677   6.5     https://vulners.com/cve/CVE-2021-3677
    CVE-2021-32029  6.5     https://vulners.com/cve/CVE-2021-32029
    CVE-2021-32028  6.5     https://vulners.com/cve/CVE-2021-32028
    CVE-2014-0065   6.5     https://vulners.com/cve/CVE-2014-0065
    CVE-2014-0064   6.5     https://vulners.com/cve/CVE-2014-0064
    CVE-2014-0063   6.5     https://vulners.com/cve/CVE-2014-0063
    CVE-2014-0061   6.5     https://vulners.com/cve/CVE-2014-0061
    CVE-2012-0866   6.5     https://vulners.com/cve/CVE-2012-0866
    CVE-2010-4015   6.5     https://vulners.com/cve/CVE-2010-4015
    CVE-2010-0442   6.5     https://vulners.com/cve/CVE-2010-0442
    CVE-2015-5288   6.4     https://vulners.com/cve/CVE-2015-5288
    CVE-2010-3433   6.0     https://vulners.com/cve/CVE-2010-3433
    CVE-2010-1170   6.0     https://vulners.com/cve/CVE-2010-1170
    CVE-2021-23222  5.9     https://vulners.com/cve/CVE-2021-23222
    SSV:19669       5.5     https://vulners.com/seebug/SSV:19669    *EXPLOIT*
    CVE-2010-1975   5.5     https://vulners.com/cve/CVE-2010-1975
    CVE-2023-2455   5.4     https://vulners.com/cve/CVE-2023-2455
    SSV:61546       4.9     https://vulners.com/seebug/SSV:61546    *EXPLOIT*
    SSV:60334       4.9     https://vulners.com/seebug/SSV:60334    *EXPLOIT*
    CVE-2014-0062   4.9     https://vulners.com/cve/CVE-2014-0062
    CVE-2012-3488   4.9     https://vulners.com/cve/CVE-2012-3488
    SSV:61544       4.6     https://vulners.com/seebug/SSV:61544    *EXPLOIT*
    CVE-2014-0067   4.6     https://vulners.com/cve/CVE-2014-0067
    CVE-2021-3393   4.3     https://vulners.com/cve/CVE-2021-3393
    CVE-2021-20229  4.3     https://vulners.com/cve/CVE-2021-20229
    CVE-2015-3165   4.3     https://vulners.com/cve/CVE-2015-3165
    CVE-2014-8161   4.3     https://vulners.com/cve/CVE-2014-8161
    CVE-2012-2143   4.3     https://vulners.com/cve/CVE-2012-2143
    SSV:61547       4.0     https://vulners.com/seebug/SSV:61547    *EXPLOIT*
    SSV:61545       4.0     https://vulners.com/seebug/SSV:61545    *EXPLOIT*
    SSV:60186       4.0     https://vulners.com/seebug/SSV:60186    *EXPLOIT*
    CVE-2014-0066   4.0     https://vulners.com/cve/CVE-2014-0066
    CVE-2014-0060   4.0     https://vulners.com/cve/CVE-2014-0060
    CVE-2012-2655   4.0     https://vulners.com/cve/CVE-2012-2655
    CVE-2009-3229   4.0     https://vulners.com/cve/CVE-2009-3229
    CVE-2022-41862  3.7     https://vulners.com/cve/CVE-2022-41862
    SSV:19322       3.5     https://vulners.com/seebug/SSV:19322    *EXPLOIT*
    PACKETSTORM:127092      3.5     https://vulners.com/packetstorm/PACKETSTORM:127092      *EXPLOIT*
    CVE-2010-0733   3.5     https://vulners.com/cve/CVE-2010-0733
    EDB-ID:33729    0.0     https://vulners.com/exploitdb/EDB-ID:33729      *EXPLOIT*
    EDB-ID:33571    0.0     https://vulners.com/exploitdb/EDB-ID:33571      *EXPLOIT*
```

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.imperialviolet.org/2014/10/14/poodle.html
    https://www.openssl.org/~bodo/ssl-poodle.pdf
    https://www.securityfocus.com/bid/70574
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
```

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-date

```
2024-09-27T19:56:24+00:00; -1s from scanner time.
```

ssl-enum-ciphers

```
SSLv3:
  ciphers:
    TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - F
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - F
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - F
    TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - F
```

```
      TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - F
      TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - F
      TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - F
    compressors:
      DEFLATE
      NULL
    cipher preference: client
    warnings:
      64-bit block cipher 3DES vulnerable to SWEET32 attack
      Broken cipher RC4 is deprecated by RFC 7465
      CBC-mode cipher in SSLv3 (CVE-2014-3566)
      Insecure certificate signature (SHA1), score capped at F
  TLSv1.0:
    ciphers:
      TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - F
      TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - F
      TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - F
      TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - F
      TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - F
      TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - F
      TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - F
    compressors:
      DEFLATE
      NULL
    cipher preference: client
    warnings:
      64-bit block cipher 3DES vulnerable to SWEET32 attack
      Broken cipher RC4 is deprecated by RFC 7465
      Insecure certificate signature (SHA1), score capped at F
  least strength: F
```

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
      http://www.openssl.org/news/secadv_20140605.txt
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
```

5900	tcp	open	vnc	syn-ac

banner

```
RFB 003.003
```

vnc-info

```
  Protocol version: 3.3
  Security types:
    VNC Authentication (2)
```

vnc-brute

```
  Accounts: No valid accounts found
  Statistics: Performed 0 guesses in 24 seconds, average tps: 0.0
```

6000	tcp	open	X11	syn-ac
6667	tcp	open	irc	syn-ac

irc-sasl-brute

```
  Accounts: No valid accounts found
  Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
  ERROR: The service seems to have failed or is heavily firewalled...
```

banner

```
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hos...
```

6697	tcp	open	irc	syn-ac

unusual-port

```
irc unexpected on port tcp/6697
```

ssl-ccs-injection

```
No reply from server (TIMEOUT)
```

irc-sasl-brute

```
  Accounts: No valid accounts found
  Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
  ERROR: The service seems to have failed or is heavily firewalled...
```

banner

```
ERROR :Closing Link: [192.168.1.101] (Too many unknown conne...
```

irc-botnet-channels

```
  ERROR: Closing Link: [192.168.1.101] (Too many unknown connections from your IP)
```

8009	tcp	open	ajp13	syn-ac

ajp-methods

```
Failed to get a valid response for the OPTION request
```

ajp-request

```
AJP/1.3 200 OK
Content-Type: text/html;charset=ISO-8859-1

iguring and using Tomcat</li>
               <li><b><a href="mailto:dev@tomcat.apache.org">dev@tomcat.apache.org</a></b> for developers working on Tomcat</li
```

```
          </ul>

           <p>Thanks for using Tomcat!</p>

           <p id="footer"><img src="tomcat-power.gif" width="77" height="80" alt="Powered by Tomcat"/><br/>
           &nbsp;

           Copyright &copy; 1999-2005 Apache Software Foundation<br/>
           All Rights Reserved
           </p>
       </td>

    </tr>
</table>

</body>
</html>
```

ajp-headers

```
  Content-Type: text/html;charset=ISO-8859-1
```

ajp-brute

```
  URL does not require authentication
```

8180	tcp	open	http	syn-ac

http-date

```
Fri, 27 Sep 2024 19:48:46 GMT; -2s from local time.
```

http-csrf

```
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.50.100
  Found the following possible CSRF vulnerabilities:

    Path: http://192.168.50.100:8180/admin/
    Form id: username
    Form action: j_security_check;jsessionid=ECE726D44B256EB36E2B32AE68757AD5

    Path: http://192.168.50.100:8180/servlets-examples/servlet/SessionExample
    Form id:
    Form action: SessionExample;jsessionid=14496932D54149D8BDC9F63A7B5D73B4

    Path: http://192.168.50.100:8180/servlets-examples/servlet/SessionExample
    Form id:
    Form action: SessionExample;jsessionid=14496932D54149D8BDC9F63A7B5D73B4

    Path: http://192.168.50.100:8180/servlets-examples/servlet/CookieExample
    Form id:
    Form action: CookieExample
```

http-slowloris

```
false
```

http-feed

```
Couldn't find any feeds.
```

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-default-accounts	[Apache Tomcat] at /manager/html/ tomcat:tomcat [Apache Tomcat Host Manager] at /host-manager/html/ tomcat:tomcat
	http-headers	Server: Apache-Coyote/1.1 Content-Type: text/html;charset=ISO-8859-1 Date: Fri, 27 Sep 2024 19:48:47 GMT Connection: close (Request type: HEAD)
	http-security-headers	
	http-stored-xss	Couldn't find any stored XSS vulnerabilities.
	http-chrono	Request times for /; avg: 1456.81ms; min: 597.78ms; max: 3909.66ms

	http-errors	Spidering limited to: maxpagecount=40; withinhost=192.168.50.100
		  Found the following error pages:
		
		  Error Code: 401
		        http://192.168.50.100:8180/manager/html
		
		  Error Code: 401
		        http://192.168.50.100:8180/manager/status

	http-sitemap-generator	Directory structure:
		    /
		      Other: 1; gif: 1
		    /admin/
		      Other: 1
		    /jsp-examples/
		      Other: 1
		    /servlets-examples/
		      Other: 1
		    /tomcat-docs/
		      Other: 1
		    /webdav/
		      Other: 1
		  Longest directory structure:
		    Depth: 1
		    Dir: /servlets-examples/
		  Total files found (by extension):
		    Other: 6; gif: 1

	http-comments-displayer	Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.50.100
		
		    Path: http://192.168.50.100:8180/
		    Line number: 84
		    Comment:
		        /*]]>*/
		
		    Path: http://192.168.50.100:8180/
		    Line number: 25
		    Comment:
		        /*<![CDATA[*/
		
		    Path: http://192.168.50.100:8180/tomcat-docs/changelog.html
		    Line number: 3690
		    Comment:
		        <!--FOOTER SEPARATOR-->
		
		    Path: http://192.168.50.100:8180/tomcat-docs/changelog.html
		    Line number: 1
		    Comment:

```
    <!--PAGE HEADER-->

Path: http://192.168.50.100:8180/servlets-examples/reqinfo.html
Line number: 55
Comment:
    /**
         * We are going to perform the same operations for POST requests
         * as for GET methods, so this method just sends the request to
         * the doGet method.
         */

Path: http://192.168.50.100:8180/servlets-examples/sessions.html
Line number: 59
Comment:
     // print session contents

Path: http://192.168.50.100:8180/
Line number: 90
Comment:
    <!-- Header -->

Path: http://192.168.50.100:8180/admin/
Line number: 36
Comment:
     // -->

Path: http://192.168.50.100:8180/admin/
Line number: 40
Comment:
    <!-- Standard Content -->

Path: http://192.168.50.100:8180/tomcat-docs/changelog.html
Line number: 3
Comment:
    <!--LEFT SIDE NAVIGATION-->

Path: http://192.168.50.100:8180/jsp-examples/
Line number: 56
Comment:
    <!--<tr VALIGN=TOP>
    <td WIDTH="30"><img SRC="images/read.gif" height=24 width=24></td>

    <td>Read more about this feature</td>
    -->

Path: http://192.168.50.100:8180/admin/
Line number: 131
Comment:
    <!--
        document.forms["loginForm"].elements["j_username"].focus()
      // -->

Path: http://192.168.50.100:8180/admin/
Line number: 1
Comment:
    <!--
      Licensed to the Apache Software Foundation (ASF) under one or more
      contributor license agreements.  See the NOTICE file distributed with
      this work for additional information regarding copyright ownership.
      The ASF licenses this file to You under the Apache License, Version 2.0
      (the "License"); you may not use this file except in compliance with
      the License.  You may obtain a copy of the License at

          http://www.apache.org/licenses/LICENSE-2.0

      Unless required by applicable law or agreed to in writing, software
      distributed under the License is distributed on an "AS IS" BASIS,
      WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
      See the License for the specific language governing permissions and
      limitations under the License.
    -->

Path: http://192.168.50.100:8180/manager/status
Line number: 1
Comment:
    <!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahom

Path: http://192.168.50.100:8180/tomcat-docs/changelog.html
Line number: 3
Comment:
    <!--HEADER SEPARATOR-->

Path: http://192.168.50.100:8180/tomcat-docs/changelog.html
Line number: 1
Comment:
    <!--PROJECT LOGO-->

Path: http://192.168.50.100:8180/jsp-examples/
Line number: 24
Comment:
    <!--
      Copyright (c) 1999 The Apache Software Foundation.  All rights
      reserved.
    -->

Path: http://192.168.50.100:8180/admin/
Line number: 138
Comment:
    <!-- Standard Footer -->

Path: http://192.168.50.100:8180/admin/
Line number: 79
Comment:
    <!-- banner -->
```

```
Path: http://192.168.50.100:8180/tomcat-docs/changelog.html
Line number: 3690
Comment:
    <!--PAGE FOOTER-->

Path: http://192.168.50.100:8180/admin/
Line number: 72
Comment:
    <!-- Login -->

Path: http://192.168.50.100:8180/admin/
Line number: 85
Comment:
    <!-- username password prompts fields layout -->

Path: http://192.168.50.100:8180/admin/
Line number: 32
Comment:
    <!--
        if (window.self != window.top) {
          window.open(".", "_top");
        }
      // -->

Path: http://192.168.50.100:8180/tomcat-docs/changelog.html
Line number: 3
Comment:
    <!--APACHE LOGO-->

Path: http://192.168.50.100:8180/admin/
Line number: 17
Comment:
    <!-- Standard Struts Entries -->

Path: http://192.168.50.100:8180/admin/
Line number: 112
Comment:
    <!-- login reset buttons layout -->

Path: http://192.168.50.100:8180/servlets-examples/reqheaders.html
Line number: 1
Comment:
    <!--
     Licensed to the Apache Software Foundation (ASF) under one or more
      contributor license agreements.  See the NOTICE file distributed with
      this work for additional information regarding copyright ownership.
      The ASF licenses this file to You under the Apache License, Version 2.0
      (the "License"); you may not use this file except in compliance with
      the License.  You may obtain a copy of the License at

          http://www.apache.org/licenses/LICENSE-2.0

      Unless required by applicable law or agreed to in writing, software
      distributed under the License is distributed on an "AS IS" BASIS,
      WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
      See the License for the specific language governing permissions and
      limitations under the License.
    -->

Path: http://192.168.50.100:8180/admin/
Line number: 66
Comment:
    <!-- Body -->

Path: http://192.168.50.100:8180/tomcat-docs/changelog.html
Line number: 3
Comment:
    <!--RIGHT SIDE MAIN BODY-->

Path: http://192.168.50.100:8180/
Line number: 110
Comment:
    <!-- Table of Contents -->

Path: http://192.168.50.100:8180/admin/
Line number: 28
Comment:
    <!-- Make sure window is not in a frame -->
```

http-referer-checker

```
Couldn't find any cross-domain scripts.
```

http-devframework

```
Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.
```

http-auth-finder

```
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.50.100
  url                                          method
  http://192.168.50.100:8180/manager/html    HTTP: Basic
  http://192.168.50.100:8180/admin/          FORM
  http://192.168.50.100:8180/manager/status  HTTP: Basic
```

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-fetch	Please enter the complete path of the directory to save data in.		
	http-mobileversion-checker	No mobile version detected.		
	http-title	Apache Tomcat/5.5		
	http-vhosts	128 names had status 200		
	http-favicon	Apache Tomcat		
	http-brute	Path "/" does not require authentication		
	http-xssed	No previously reported XSS vuln.		
	http-dombased-xss	Couldn't find any DOM based XSS.		
	http-useragent-tester	Status for browser useragent: 200 Allowed User Agents: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html) libwww lwp-trivial libcurl-agent/1.0 PHP/ Python-urllib/2.5 GT::WWW Snoopy MFC_Tear_Sample HTTP::Lite PHPCrawl URI::Fetch Zend_Http_Client http client PECL::HTTP Wget/1.13.4 (linux-gnu) WWW-Mechanize/1.34		
	http-grep	(2) http://192.168.50.100:8180/: (2) email: + users@tomcat.apache.org + dev@tomcat.apache.org (3) http://192.168.50.100:8180/tomcat-docs/: (3) email: + craigmcc@apache.org + remm@apache.org + yoavs@apache.org (1) http://192.168.50.100:8180/admin/: (1) ip: + 192.168.50.100		
8787	tcp	open	drb	syn-ac
	unusual-port	drb unexpected on port tcp/8787		
34181	tcp	open	mountd	syn-ac
	nfs-showmount	/ *		
40607	tcp	open	nlockmgr	syn-ac
47589	tcp	open	status	syn-ac
59950	tcp	open	java-rmi	syn-ac
	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		

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **34064/udp** (**closed**)
- OS match: **Linux 2.6.15 - 2.6.26 (likely embedded)** (**100%**)
- OS match: **Linux 2.6.29 (Gentoo)** (**100%**)

Host Script Output

Script Name	Output
smb-vuln-ms10-061	false
smb-enum-users	Domain: METASPLOITABLE; Users: backup, bin, bind, daemon, dhcp, distccd, ftp, games, gnats, irc, klog, libuuid, list, lp, mail, man,
smb-print-text	false
smb-vuln-ms10-054	false
smb-security-mode	account_used: msfadmin authentication_level: user challenge_response: supported message_signing: disabled (dangerous, but default)
nfs-ls	Volume / access: Read Lookup Modify Extend Delete NoExecute PERMISSION UID GID SIZE TIME FILENAME -rw-r--r-- 0 0 0 2024-09-23T18:00:51 GBTJL\x03} drwxr-xr-x 0 0 4096 2012-05-14T03:35:33 bin drwxr-xr-x 0 0 4096 2010-04-16T06:16:02 home drwxr-xr-x 0 0 4096 2010-03-16T22:57:40 initrd lrwxrwxrwx 0 0 32 2010-04-28T20:26:18 initrd.img drwxr-xr-x 0 0 4096 2012-05-14T03:35:22 lib drwx------ 0 0 16384 2010-03-16T22:55:15 lost+found drwxr-xr-x 0 0 4096 2010-03-16T22:55:52 media drwxr-xr-x 0 0 4096 2010-04-28T20:16:56 mnt drwxr-xr-x 0 0 4096 2012-05-14T01:54:53 sbin
smb2-time	Protocol negotiation failed (SMB2)
msrpc-enum	NT_STATUS_OBJECT_NAME_NOT_FOUND
smb-brute	msfadmin:msfadmin => Valid credentials user:user => Valid credentials
smb-protocols	dialects: NT LM 0.12 (SMBv1) [dangerous, but default]
smb-system-info	ERROR: Script execution failed (use -d to debug)
smb-os-discovery	OS: Unix (Samba 3.0.20-Debian) Computer name: metasploitable NetBIOS computer name: Domain name: localdomain FQDN: metasploitable.localdomain System time: 2024-09-27T15:54:45-04:00
dns-brute	Can't guess domain of "192.168.50.100"; use dns-brute.domain script argument.

port-states	tcp:
	  open: 21-23,25,53,80,111,139,445,512-514,1099,1524,2049,2121,3306,3632,5432,5900,6000,6667,6697,8009,8180,8787,34181,40607,47589,59
	  filtered: 422,954,1409,1604,2882,2902,3102,3259,3865,4724,5091,5345,6370,6658,7225,7322,7425,7489,7801,7925,8731,8904,9586,10153,10
	  closed: 1-20,24,26-52,54-79,81-110,112-138,140-421,423-444,446-511,515-953,955-1098,1100-1408,1410-1523,1525-1603,1605-2048,2050-21

traceroute-geolocation	HOP RTT ADDRESS GEOLOCATION 1 1.45 pfSense.home.arpa (192.168.1.1) - ,- 2 3.55 192.168.50.100 - ,-
qscan	PORT FAMILY MEAN (us) STDDEV LOSS (%) 1 0 2206.80 307.29 0.0% 21 0 2506.60 512.50 0.0% 22 0 2498.90 516.97 0.0% 23 0 2465.00 657.91 0.0% 25 1 2494.80 396.83 0.0% 53 0 2371.90 433.21 0.0% 80 1 2561.80 497.23 0.0% 111 0 2368.00 211.35 0.0% 139 0 2396.90 502.34 0.0%

ipidseq

```
All zeros
```

path-mtu

```
PMTU == 1500
```

smb-enum-shares

```
  account_used: msfadmin
  \\192.168.50.100\ADMIN$:
    Type: STYPE_IPC
    Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
    Users: 1
    Max Users: <unlimited>
    Path: C:\tmp
    Anonymous access: <none>
    Current user access: READ/WRITE
  \\192.168.50.100\IPC$:
    Type: STYPE_IPC
    Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
    Users: 1
    Max Users: <unlimited>
    Path: C:\tmp
    Anonymous access: READ/WRITE
    Current user access: READ/WRITE
  \\192.168.50.100\msfadmin:
    Type: STYPE_DISKTREE
    Comment: Home Directories
    Users: 1
    Max Users: <unlimited>
    Path: C:\home\msfadmin
    Anonymous access: <none>
    Current user access: READ/WRITE
  \\192.168.50.100\opt:
    Type: STYPE_DISKTREE
    Comment:
    Users: 1
    Max Users: <unlimited>
    Path: C:\tmp
    Anonymous access: <none>
    Current user access: READ/WRITE
  \\192.168.50.100\print$:
    Type: STYPE_DISKTREE
    Comment: Printer Drivers
    Users: 1
    Max Users: <unlimited>
    Path: C:\var\lib\samba\printers
    Anonymous access: <none>
    Current user access: READ/WRITE
  \\192.168.50.100\tmp:
    Type: STYPE_DISKTREE
    Comment: oh noes!
    Users: 1
    Max Users: <unlimited>
    Path: C:\tmp
    Anonymous access: READ
    Current user access: READ/WRITE
```

fcrdns

```
FAIL (No PTR record)
```

nbstat

```
NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

smb-ls

```
Volume \\192.168.50.100\msfadmin
SIZE   TIME                 FILENAME
<DIR>  2024-09-27T19:55:53  .
<DIR>  2010-04-16T06:16:02  ..
13     2024-09-07T07:11:37  giggino.txt.save
<DIR>  2010-04-28T03:44:17  vulnerable
<DIR>  2010-04-28T06:48:36  vulnerable\samba
<DIR>  2010-04-28T07:12:05  vulnerable\mysql-ssl
<DIR>  2010-04-16T20:37:02  vulnerable\twiki20030201
<DIR>  2010-04-19T23:43:18  vulnerable\tikiwiki


Volume \\192.168.50.100\opt
SIZE   TIME                 FILENAME
<DIR>  2024-09-27T19:55:58  .
<DIR>  2024-09-23T18:00:51  ..
0      2024-09-27T16:59:11  4570.jsvc_up
260    2024-09-27T19:55:14  nmap-test-file


Volume \\192.168.50.100\print$
SIZE   TIME                 FILENAME
<DIR>  2010-04-28T06:51:21  .
<DIR>  2010-04-28T06:51:22  ..
<DIR>  2010-04-28T06:33:43  W32X86
<DIR>  2010-04-28T06:33:43  WIN40


Volume \\192.168.50.100\tmp
SIZE   TIME                 FILENAME
<DIR>  2024-09-27T19:58:40  .
<DIR>  2024-09-23T18:00:51  ..
0      2024-09-27T16:59:11  4570.jsvc_up
260    2024-09-27T19:55:14  nmap-test-file
```

firewalk

```
HOP  HOST         PROTOCOL  BLOCKED PORTS
1    192.168.1.1  tcp       422,954,1409,1604,2882,2902,3102,3259,3865,4724
```

smb-mbenum

```
Master Browser
  METASPLOITABLE  0.0  metasploitable server (Samba 3.0.20-Debian)
Print server
  METASPLOITABLE  0.0  metasploitable server (Samba 3.0.20-Debian)
Server
  METASPLOITABLE  0.0  metasploitable server (Samba 3.0.20-Debian)
Server service
  METASPLOITABLE  0.0  metasploitable server (Samba 3.0.20-Debian)
Unix server
  METASPLOITABLE  0.0  metasploitable server (Samba 3.0.20-Debian)
Windows NT/2000/XP/2003 server
  METASPLOITABLE  0.0  metasploitable server (Samba 3.0.20-Debian)
Workstation
  METASPLOITABLE  0.0  metasploitable server (Samba 3.0.20-Debian)
```

dns-blacklist

```
SPAM
  l2.apews.org - FAIL
```

smb-enum-sessions

```
ERROR: Script execution failed (use -d to debug)
```

nfs-statfs

```
Filesystem  1K-blocks  Used       Available  Use%  Maxfilesize  Maxlink
/           7282168.0  1500192.0  5414976.0  22%   2.0T         32000
```

smb2-capabilities

```
SMB 2+ not supported
```

smb-flood

```
ERROR: Script execution failed (use -d to debug)
```

smb-vuln-regsvc-dos

```
ERROR: Script execution failed (use -d to debug)
```

clock-skew

```
mean: 47m58s, deviation: 1h47m20s, median: -2s
```

Traceroute Information

- Traceroute data generated using port 587/tcp

Hop	Rtt	IP	Host
1	1.45	192.168.1.1	pfSense.home.arpa
2	3.55	192.168.50.100	

Misc Metrics

Metric	Value
Ping Results	echo-reply
System Uptime	10534 seconds (last reboot: Fri Sep 27 13:03:40 2024)
Network Distance	2 hops
TCP Sequence Prediction	Difficulty=204 (Good luck!)
IP ID Sequence Generation	All zeros

Post-Scan Script Output

Script Name — **Output**

reverse-index

```
21/tcp: 192.168.50.100
22/tcp: 192.168.50.100
23/tcp: 192.168.50.100
25/tcp: 192.168.50.100
53/tcp: 192.168.50.100
80/tcp: 192.168.50.100
111/tcp: 192.168.50.100
139/tcp: 192.168.50.100
445/tcp: 192.168.50.100
512/tcp: 192.168.50.100
513/tcp: 192.168.50.100
514/tcp: 192.168.50.100
1099/tcp: 192.168.50.100
1524/tcp: 192.168.50.100
2049/tcp: 192.168.50.100
2121/tcp: 192.168.50.100
3306/tcp: 192.168.50.100
3632/tcp: 192.168.50.100
5432/tcp: 192.168.50.100
5900/tcp: 192.168.50.100
6000/tcp: 192.168.50.100
6667/tcp: 192.168.50.100
6697/tcp: 192.168.50.100
8009/tcp: 192.168.50.100
8180/tcp: 192.168.50.100
8787/tcp: 192.168.50.100
34181/tcp: 192.168.50.100
40607/tcp: 192.168.50.100
47589/tcp: 192.168.50.100
59950/tcp: 192.168.50.100
```

creds-summary

```
192.168.50.100:
  8180/http:
```

```
tomcat:tomcat - Valid credentials
tomcat:tomcat - Valid credentials
```