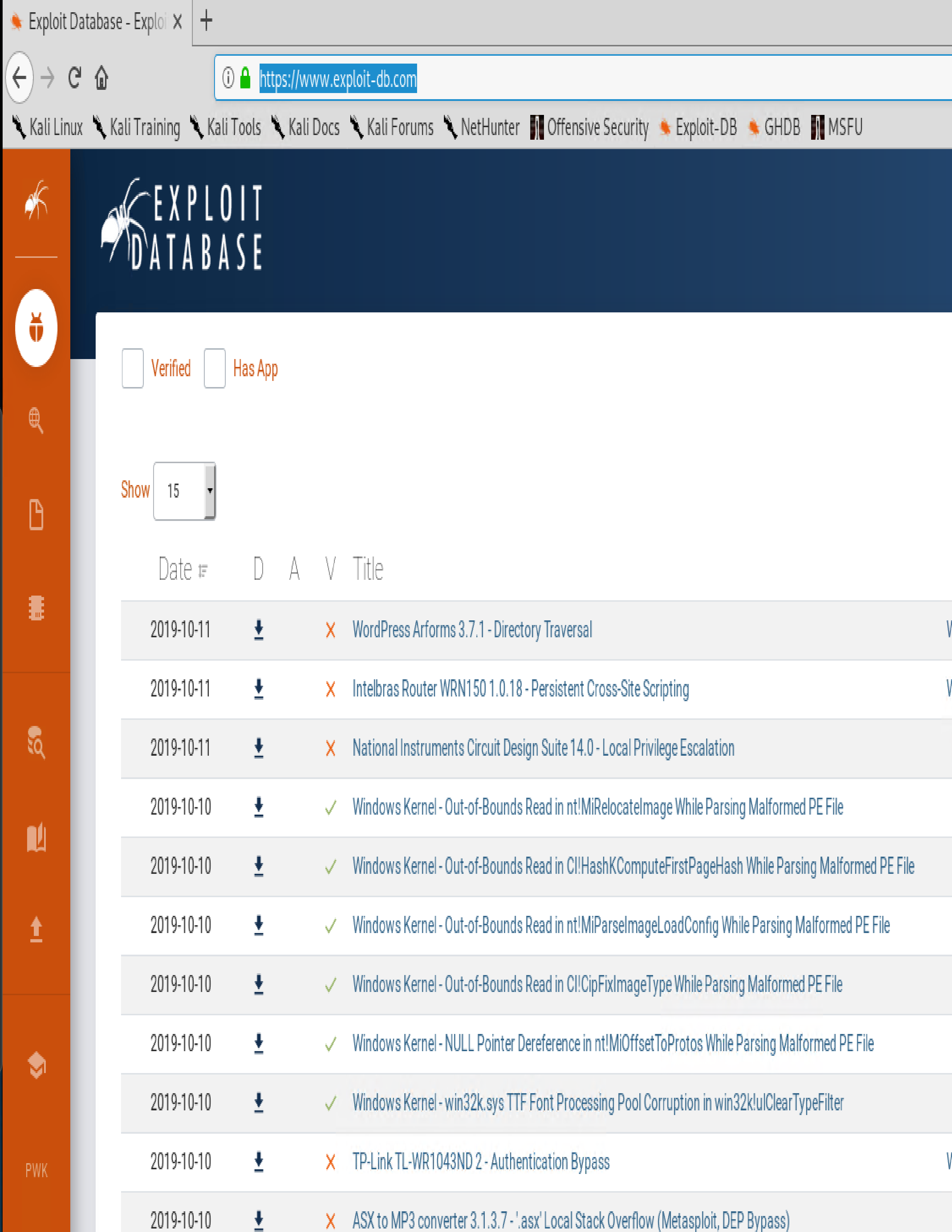
```
[i] Database already started
[i] The database appears to be already configured, skipping initialization

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;.  .;P'  '.'  /  |  \  `.'
  II      'T; ;P'     `. /   |   \ .'
IIIIII     'YvP'        `-.__|__.-'

I love shells --egypt

       =[ metasploit v5.0.41-dev                          ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 >
```

Whats we can DO with MetaSploit?

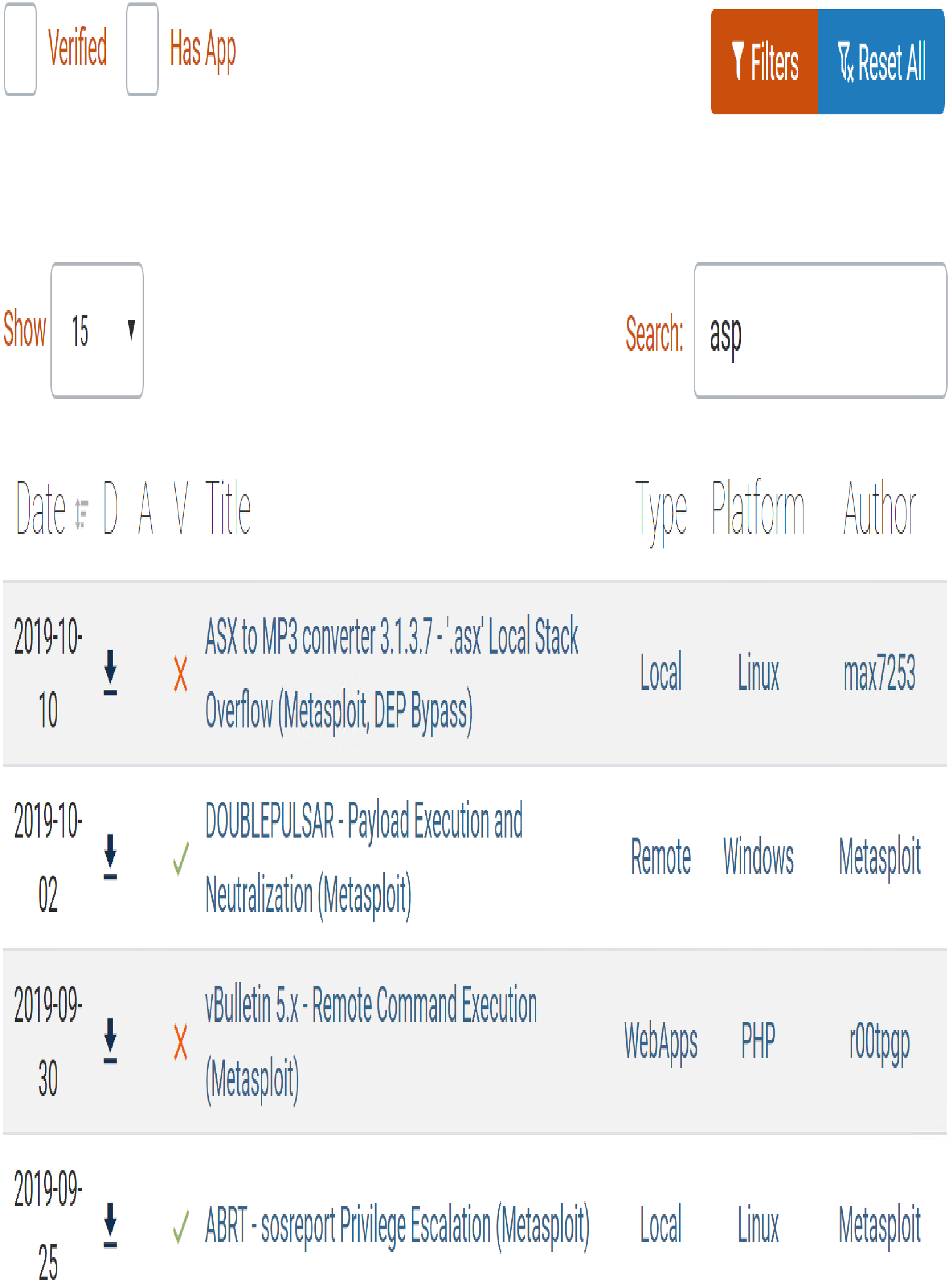
NullByte



□ Verified □ Has App

Show 15

Date	D	A	V	Title
2019-10-11	⬇		✗	WordPress Arforms 3.7.1 - Directory Traversal
2019-10-11	⬇		✗	Intelbras Router WRN150 1.0.18 - Persistent Cross-Site Scripting
2019-10-11	⬇		✗	National Instruments Circuit Design Suite 14.0 - Local Privilege Escalation
2019-10-10	⬇		✓	Windows Kernel - Out-of-Bounds Read in nt!MiRelocateImage While Parsing Malformed PE File
2019-10-10	⬇		✓	Windows Kernel - Out-of-Bounds Read in CI!HashKComputeFirstPageHash While Parsing Malformed PE File
2019-10-10	⬇		✓	Windows Kernel - Out-of-Bounds Read in nt!MiParseImageLoadConfig While Parsing Malformed PE File
2019-10-10	⬇		✓	Windows Kernel - Out-of-Bounds Read in CI!CipFixImageType While Parsing Malformed PE File
2019-10-10	⬇		✓	Windows Kernel - NULL Pointer Dereference in nt!MiOffsetToProtos While Parsing Malformed PE File
2019-10-10	⬇		✓	Windows Kernel - win32k.sys TTF Font Processing Pool Corruption in win32k!ulClearTypeFilter
2019-10-10	⬇		✗	TP-Link TL-WR1043ND 2 - Authentication Bypass
2019-10-10	⬇		✗	ASX to MP3 converter 3.1.3.7 - '.asx' Local Stack Overflow (Metasploit, DEP Bypass)



□ Verified □ Has App

Filters | Reset All

Show 15 ▾

Search: asp

Date	D	A	V	Title	Type	Platform	Author
2019-10-10	⬇		✗	ASX to MP3 converter 3.1.3.7 - '.asx' Local Stack Overflow (Metasploit, DEP Bypass)	Local	Linux	max7253
2019-10-02	⬇		✓	DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)	Remote	Windows	Metasploit
2019-09-30	⬇		✗	vBulletin 5.x - Remote Command Execution (Metasploit)	WebApps	PHP	r00tpgp
2019-09-25	⬇		✓	ABRT - sosreport Privilege Escalation (Metasploit)	Local	Linux	Metasploit

Author:	Type:
METASPLOIT	REMOTE

Exploit: ⬇ / {}

```
class MetasploitModule < Msf::Exploit::Remote

  Rank = GreatRanking

  include Msf::Exploit::Remote::SMB::Client

  MAX_SHELLCODE_SIZE = 4096

  def initialize(info = {})
    super(update_info(info,
      'Name'                => 'DOUBLEPULSAR Payload Execut
Neutralization',
      'Description'         => %q{
        This module executes a Metasploit payload agains
Equation Group's
        DOUBLEPULSAR implant for SMB as popularly deploy
ETERNALBLUE.
```