Network Scan Assessment Report

Nmap Scan Summary for 150.1.7.0/24

Scan started at: Sun Jun 29 12:15:53 PM EDT 2025

==========

Host: 150.1.7.100

| Port | State | Service | Version |

|------|-------|---------|---------|

| 135/tcp | open | msrpc | msrpc Microsoft Windows RPC |

| 139/tcp | open | netbios-ssn | netbios-ssn Microsoft Windows netbios-ssn |

| 445/tcp | open | microsoft-ds? | microsoft-ds? |

| 5357/tcp | open | http | http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |

| |_http-server-header: | Microsoft-HTTPAPI/2.0 | | |

| 7070/tcp | open | ssl/realserver? | ssl/realserver? |

| MAC | Address: | 00:50:56:C0:00:01 | (VMware) |

| Warning: | OSScan | results | may be unreliable because we could not find at least 1 open and 1 closed port |

| Device | type: | general | purpose |

| Running | (JUST | GUESSING): | Microsoft Windows 10|11|2019 (97%) |

| OS | CPE: | cpe:/o:microsoft:windows_10 | cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2019 |

| Aggressive | OS | guesses: | Microsoft Windows 10 1803 (97%), Microsoft Windows 10 1903 - 21H1 (97%), Microsoft Windows 11 (92%), Microsoft Windows 10 1909 (91%), Microsoft Windows 10 1909 - 2004 (91%), Windows Server 2019 (91%), Microsoft Windows 10 1809 (91%), Microsoft Windows 10 20H2 (88%) |

| No | exact | OS | matches for host (test conditions non-ideal). |

| Network | Distance: | 1 | hop |

| Service | Info: | OS: | Windows; CPE: cpe:/o:microsoft:windows |

==========

Host: 150.1.7.102

| Port | State | Service | Version |

|---|---|---|---|

| 80/tcp | open | http | open http Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12) |

| |_http-server-header: | Apache/2.4.58 | (Win64) | OpenSSL/3.1.3 PHP/8.2.12 |

| 135/tcp | open | msrpc | msrpc Microsoft Windows RPC |

| 139/tcp | open | netbios-ssn | netbios-ssn Microsoft Windows netbios-ssn |

| 443/tcp | open | ssl/http | ssl/http Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12) |

| |_http-server-header: | Apache/2.4.58 | (Win64) | OpenSSL/3.1.3 PHP/8.2.12 |

| 445/tcp | open | microsoft-ds? | microsoft-ds? |

| 3306/tcp | open | mysql | mysql MariaDB 10.3.23 or earlier (unauthorized) |

| | | banner: | F\x00\x00\x00\xFFj\x04Host | '150.1.7.101' is not allowed to conn |

| |_ect | to | this | MariaDB server |

| MAC | Address: | 00:0C:29:2B:8B:98 | (VMware) |

| Device | type: | general | purpose |

| Running: | Microsoft | Windows | 10 |

| OS | CPE: | cpe:/o:microsoft:windows_10 | |

| OS | details: | Microsoft | Windows 10 1709 - 21H2 |

| Network | Distance: | 1 | hop |

| Service | Info: | OS: | Windows; CPE: cpe:/o:microsoft:windows |

==========

Host: 150.1.7.104

| Port | State | Service | Version |

|------|-------|---------|---------|

| 21/tcp | open | ftp | open ftp vsftpd 2.3.4 |

| |_banner: | 220 | (vsFTPd | 2.3.4) |

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

| |_banner: | SSH-2.0-OpenSSH_4.7p1 | Debian-8ubuntu1 | |

| 23/tcp | open | telnet | open telnet Linux telnetd |

| |_banner: | \xFF\xFD\x18\xFF\xFD | \xFF\xFD#\xFF\xFD' | |

| 25/tcp | open | smtp | open smtp Postfix smtpd |

| |_banner: | 220 | metasploitable.localdomain | ESMTP Postfix (Ubuntu) |

| 53/tcp | open | domain | open domain ISC BIND 9.4.2 |

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

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

| 111/tcp | open | rpcbind | rpcbind 2 (RPC #100000) |

| | | rpcinfo: | | |

| | | program | version | program version port/proto service |

| | | 100000 | 2 | 100000 2 111/tcp rpcbind |

| | | 100000 | 2 | 100000 2 111/udp rpcbind |

| | | 100003 | 2,3,4 | 100003 2,3,4 2049/tcp nfs |

| | | 100003 | 2,3,4 | 100003 2,3,4 2049/udp nfs |

| | | 100005 | 1,2,3 | 100005 1,2,3 42270/udp mountd |

| | | 100005 | 1,2,3 | 100005 1,2,3 59865/tcp mountd |

| | | 100021 | 1,3,4 | 100021 1,3,4 53129/udp nlockmgr |

| | | 100021 | 1,3,4 | 100021 1,3,4 54253/tcp nlockmgr |

```
| |    | 100024 | 1       | 100024  1          51644/udp   status |

| |_   | 100024 | 1       |  1          59447/tcp   status |

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

| 445/tcp | open  | netbios-ssn |  netbios-ssn Samba smbd 3.X - 4.X
(workgroup: WORKGROUP) |

| 513/tcp | open  | login    |  login       OpenBSD or Solaris rlogind |

| 514/tcp | open  | tcpwrapped |  tcpwrapped |

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

| 2121/tcp | open  | ftp     | ftp         ProFTPD 1.3.1 |

| |_banner: | 220   | ProFTPD | 1.3.1 Server (Debian)
[::ffff:150.1.7.104] |

| 3306/tcp | open  | mysql   | mysql       MySQL 5.0.51a-3ubuntu5 |

| |    | banner: | >\x00\x00\x00\x0A5.0.51a-
3ubuntu5\x00\x0E\x00\x00\x00$Vf{Z0|F\x |         |

|
|_00,\xAA\x08\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\.
.. |       |         |
|_00,\xAA\x08\x02\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\.
.. |

| 5432/tcp | open  | postgresql | postgresql  PostgreSQL DB 8.3.0 -
8.3.7 |

| 5900/tcp | open  | vnc     | vnc         VNC (protocol 3.3) |

| |_banner: | RFB   | 003.003 |         |

| 6000/tcp | open  | X11     | X11         (access denied) |

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

| MAC  | Address: | 00:0C:29:FA:DD:34 | (VMware) |

| Device | type: | general | purpose |

| Running: | Linux | 2.6.X   |         |

| OS   | CPE:  | cpe:/o:linux:linux_kernel:2.6 |         |

| OS   | details: | Linux   | 2.6.9 - 2.6.33 |
```

| Network | Distance: | 1 | hop |

| Service | Info: | Host: | metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel |

--- Live Hosts ---

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-29 12:15 EDT

Nmap scan report for 150.1.7.100

Host is up (0.00030s latency).

MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 150.1.7.102

Host is up (0.00051s latency).

MAC Address: 00:0C:29:2B:8B:98 (VMware)

Nmap scan report for 150.1.7.104

Host is up (0.00059s latency).

MAC Address: 00:0C:29:FA:DD:34 (VMware)

Nmap scan report for 150.1.7.101

Host is up.

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.81 seconds
```

--- CVEs Found ---

Port: 111

```
---------------------------------------------------------------------------------------- ----------
----------
Exploit Title
|  Path

---------------------------------------------------------------------------------------- ----------
----------
(GREEZLE) Global Real Estate Agent Login - Multiple SQL Injections
| multiple/webapps/34[01;31m[K111[m[K.txt
```

Adobe Acrobat and Reader 8.1.1 - Multiple Arbitrary Code Execution / Security Vulnerabilities | windows/dos/3[01;31m[K111[m[K4.txt

Adobe GetPlus get_atlcom 1.6.2.48 - ActiveX Remote Execution | windows/remote/[01;31m[K111[m[K72.html

AIOCP 1.4 - 'cp_html2txt.php' Remote File Inclusion | php/webapps/33[01;31m[K111[m[K.txt

al3jeb script - Remote Authentication Bypass | php/webapps/[01;31m[K111[m[K98.txt

al3jeb script - Remote Change Password | php/webapps/[01;31m[K111[m[K85.html

Alice Modem [01;31m[K111[m[K1 - 'rulename' Cross-Site Scripting / Denial of Service | hardware/dos/35939.txt

Allomani Super MultiMedia 2.5 - Cross-Site Request Forgery (Add Admin) | php/webapps/14[01;31m[K111[m[K.txt

Alwjeez Script - Database Backup | php/webapps/[01;31m[K111[m[K16.html

Amtote Homebet - Account Information Brute Force | multiple/remote/2[01;31m[K111[m[K6.pl

AmTote Homebet - World Accessible Log | multiple/remote/2[01;31m[K111[m[K5.pl

AOL 9.5 - ActiveX Heap Overflow | windows/dos/[01;31m[K111[m[K90.txt

Apple iTunes 8.1.x - 'daap' Remote Buffer Overflow | windows/remote/[01;31m[K111[m[K38.c

Apple Mac OSX 10.3.8 - 'CF_CHARSET_PATH' Local Buffer Overflow (2) | osx/local/2[01;31m[K111[m[K.pl

Aqua Real 1.0/2.0 - Local Crash (PoC) | windows/dos/[01;31m[K111[m[K50.txt

Asp VevoCart Control System 3.0.4 - Database Disclosure | asp/webapps/[01;31m[K111[m[K34.txt

Audiotran 1.4.1 - '.pls' Local Stack Overflow (Metasploit) | windows/local/[01;31m[K111[m[K09.rb

Audiotran 1.4.1 - Direct RET Buffer Overflow | windows/local/[01;31m[K111[m[K71.pl

B2B Script 4.27 - SQL Injection
| php/webapps/4[01;31m[K111[m[K6.txt

BS.Player 2.51 - Overwrite (SEH)
| windows/local/[01;31m[K111[m[K46.py

BS.Player 2.51 - Universal Overflow (SEH)
| windows/local/[01;31m[K111[m[K54.py

Calendarix 0.8.2007[01;31m[K111[m[K8 - Multiple SQL Injections / Cross-Site Scripting Vulnerabilities |
php/webapps/25778.txt

Calendarix 0.8.2007[01;31m[K111[m[K8 - SQL Injection
| php/webapps/11443.txt

Cerberus FTP Server 4.0.9.8 - Remote Buffer Overflow
| windows/remote/36[01;31m[K111[m[K.py

CHETCPASSWD 1.12 - Shadow File Disclosure
| cgi/webapps/22[01;31m[K111[m[K.pl

CiviCRM 3.1 < Beta 5 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K111[m[K24.txt

CLONEBID B2B Marketplace - Multiple Vulnerabilities
| php/webapps/[01;31m[K111[m[K62.txt

CMScontrol 7.x - Arbitrary File Upload
| php/webapps/[01;31m[K111[m[K04.txt

Courier Management System - SQL Injection
| php/webapps/4[01;31m[K111[m[K3.txt

CuteFlow 2.11.2 - Arbitrary File Upload (Metasploit)
| php/webapps/20[01;31m[K111[m[K.rb

D-Link Routers - Authentication Bypass (2)
| hardware/webapps/[01;31m[K111[m[K01.txt

DasForum - 'layout' Local File Inclusion
| php/webapps/[01;31m[K111[m[K59.txt

DevTracker Module For bcoos 1.1.11 and E-xoops 1.0.8 - Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/3[01;31m[K111[m[K2.txt

doitX 1.0 - 'search' SQL Injection
| php/webapps/46[01;31m[K111[m[K.txt

dokuwiki 2009-12-25 - Multiple Vulnerabilities
| php/webapps/[01;31m[K111[m[K41.txt

Download Management 1.00 for PHP-Fusion - Multiple Local File Inclusions |
php/webapps/3[01;31m[K111[m[K1.txt

Dr. Web Control Center 6.00.3.20[01;31m[K111[m[K1300 - Cross-Site Scripting |
windows/webapps/20124.txt

Ebay Clone from clone2009 - SQL Injection
| php/webapps/[01;31m[K111[m[K64.txt

EFS Software Easy Chat Server 2.2 - Remote Buffer Overflow
| windows/remote/[01;31m[K111[m[K79.rb

EFTP Server 2.0.7.337 - Directory Existence / File Existence
| windows/remote/2[01;31m[K111[m[K0.pl

EggBlog 2.0 - 'message' Cross-Site Scripting
| php/webapps/27[01;31m[K111[m[K.txt

Exam Hall Management System 1.0 - Unrestricted File Upload + RCE (Unauthenticated) |
php/webapps/50[01;31m[K111[m[K.py

F*EX 20100208/20[01;31m[K111[m[K129-2 - Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/36851.txt

FAQEngine 4.24.00 - Remote File Inclusion
| php/webapps/[01;31m[K111[m[K11.txt

Fatwiki (fwiki) 1.0 - Remote File Inclusion
| php/webapps/[01;31m[K111[m[K88.txt

FirePass SSL VPN - Local File Inclusion
| multiple/webapps/23[01;31m[K111[m[K.txt

Flippa Website Script - SQL Injection
| php/webapps/4[01;31m[K111[m[K4.txt

Foxit Reader 3.1.4.1125 - ActiveX Heap Overflow (PoC)
| windows/dos/[01;31m[K111[m[K96.html

FreeBSD 4.3/4.4 - Login Capabilities Privileged File Reading
| freebsd/local/2[01;31m[K111[m[K4.txt

FreePBX 2.5.1 - SQL Injection
| multiple/webapps/[01;31m[K111[m[K86.txt

FreePBX 2.5.x - Information Disclosure
| multiple/webapps/[01;31m[K111[m[K87.txt

FreePBX 2.5.x < 2.6.0 - Persistent Cross-Site Scripting
| multiple/webapps/[01;31m[K111[m[K84.txt

GlobalLink 2.6.1.2 - 'HanGamePlugincn18.dll' ActiveX Control Multiple Buffer Overflow Vulnerabilities |
windows/remote/3[01;31m[K111[m[K3.html

Google Chrome Browser [01;31m[K111[m[K.0.5563.64 - AXPlatformNodeCocoa Fatal OOM/Crash (macOS) |
macos/local/51361.txt

Google SketchUp 7.1.6087 - 'lib3ds' 3DS Importer Memory Corruption
| windows/local/[01;31m[K111[m[K52.py

Grandora Rialto 1.6 - 'searchkey.asp' Multiple SQL Injections
| asp/webapps/29[01;31m[K111[m[K.txt

GraphicsMagick - Memory Disclosure / Heap Overflow
| multiple/dos/43[01;31m[K111[m[K.py

Gravity Board X 1.1 - CSS Template Unauthorized Access
| php/webapps/26[01;31m[K111[m[K.txt

gridcc script 1.0 - SQL Injection / Cross-Site Scripting
| php/webapps/[01;31m[K111[m[K07.txt

Hashicorp Consul v1.0 - Remote Command Execution (RCE)
| multiple/remote/5[01;31m[K111[m[K7.txt

Hesk Help Desk 2.1 - Cross-Site Request Forgery
| php/webapps/[01;31m[K111[m[K27.txt

Hikvision IP Cameras 4.1.0 b130[01;31m[K111[m[K - Multiple Vulnerabilities |
hardware/webapps/27402.txt

Hosting Controller 6.1 HotFix 2.2 - Add Domain without Quota
| asp/webapps/[01;31m[K111[m[K2.txt

HP JetDirect J3[01;31m[K111[m[KA - Invalid FTP Command Denial of Service |
hardware/dos/20090.txt

HP JetDirect rev. G.08.x/rev. H.08.x/x.08.x/J3[01;31m[K111[m[KA - LCD Display Modification |
hardware/remote/20565.c

HP OpenView OmniBack II - Generic Remote Command Execution
| multiple/remote/[01;31m[K111[m[K4.c

HTMLDOC 1.9.x-r1629 (Windows x86) - '.html' Local Buffer Overflow
| windows_x86/local/[01;31m[K111[m[K12.c

IBM Domino Web Access Upload Module - Overwrite (SEH)
| windows/remote/5[01;31m[K111[m[K.html

iBooking v1.0.8 - Arbitrary File Upload
| php/webapps/5[01;31m[K111[m[K9.txt

Image Hosting Script - Arbitrary File Upload
| php/webapps/[01;31m[K111[m[K10.txt

Insky CMS 006-0[01;31m[K111[m[K - Multiple Remote File Inclusions
| php/webapps/11848.txt

Intruder Client 1.00 - Remote Command Execution / Denial of Service
| windows/remote/[01;31m[K111[m[K5.pl

iOS Udisk FTP Basic Edition - Remote Denial of Service
| ios/dos/[01;31m[K111[m[K17.py

Ipswitch WS_FTP Server 6 - '/WSFTPSVR/FTPLogServer/LogViewer.asp'
Authentication Bypass |
asp/webapps/3[01;31m[K111[m[K7.txt

ISC BIND (Linux/BSD) - Remote Buffer Overflow (1)
| linux/remote/19[01;31m[K111[m[K.c

ITechSctipts Alibaba Clone - Multiple Vulnerabilities
| php/webapps/[01;31m[K111[m[K63.txt

Jenkins Dependency Graph View Plugin 0.13 - Persistent Cross-Site
Scripting |
java/webapps/47[01;31m[K111[m[K.txt

Jobbr 2.2.7 - Multiple SQL Injections
| php/webapps/9[01;31m[K111[m[K.txt

Joomla! Component com_articlemanager - SQL Injection
| php/webapps/[01;31m[K111[m[K40.txt

Joomla! Component com_libros - SQL Injection
| php/webapps/[01;31m[K111[m[K78.txt

Joomla! Component com_pc - Local File Inclusion
| php/webapps/[01;31m[K111[m[K68.txt

Joomla! Component com_prime - Directory Traversal
| php/webapps/[01;31m[K111[m[K77.txt

Joomla! Component com_webeecomment 2.0 - Local File Inclusion
| php/webapps/12[01;31m[K111[m[K.txt

Joomla! Component Form Maker 3.6.12 - SQL Injection
| php/webapps/44[01;31m[K111[m[K.txt

Joomla! Component Guru Pro - 'Itemid' SQL Injection
| php/webapps/40[01;31m[K111[m[K.txt

Kite 1.2020.[01;31m[K111[m[K9.0 - 'KiteService' Unquoted Service Path
| windows/local/49205.txt

KiteService 1.2020.[01;31m[K111[m[K3.1 - 'KiteService.exe' Unquoted
Service Path |
windows/local/49047.txt

Layout CMS 1.0 - SQL Injection / Cross-Site Scripting
| php/webapps/[01;31m[K111[m[K20.txt

Magic Winmail Server 4.0 (Build [01;31m[K111[m[K2) - 'download.php'
Traversal Arbitrary File Access |
php/webapps/25064.txt

Magic Winmail Server 4.0 (Build [01;31m[K111[m[K2) - 'upload.php'
Traversal Arbitrary File Upload |
php/webapps/25065.txt

Max's File Uploader - Arbitrary File Upload
| php/webapps/[01;31m[K111[m[K47.txt

Max's Image Uploader - Arbitrary File Upload
| php/webapps/[01;31m[K111[m[K69.txt

MediaMonkey 3.2.0 - Local Denial of Service
| windows/dos/[01;31m[K111[m[K65.pl

Microsoft Exchange Active Directory Topology
15.02.[01;31m[K111[m[K8.007 - 'Service MSExchangeADTopology' Unquoted
Serv | windows/local/51212.txt

Microsoft Index Server 2.0 - File Information / Full Path Disclosure
| windows/remote/2[01;31m[K111[m[K3.txt

Microsoft Internet Explorer - 'wshom.ocx' ActiveX Control Remote Code
Execution |
windows/remote/[01;31m[K111[m[K51.html

Microsoft Internet Explorer / MSN - ICC Profiles Crash (PoC)
| windows/dos/[01;31m[K111[m[K0.txt

Microsoft Internet Explorer 5 - Zone Spoofing (MS01-055)
| windows/remote/2[01;31m[K111[m[K8.txt

Microsoft Internet Explorer 6 - 'Aurora' Memory Corruption (MS10-002)
| windows/remote/[01;31m[K111[m[K67.py

Microsoft Internet Explorer 6/7/8 - Shockwave Flash Object Denial of
Service |
windows/dos/[01;31m[K111[m[K82.txt

Microsoft Windows - Color Management Module Overflow (MS05-036) (1)
| windows/dos/[01;31m[K111[m[K6.c

Microsoft Windows - NtCreateLowBoxToken Handle Capture Local Denial of Service / Privilege Escalation (MS1 | windows/dos/38580.txt

Microsoft Windows - RegLoadAppKey Hive Enumeration Privilege Escalation (MS16-[01;31m[K111[m[K) |
windows/local/40430.cs

Microsoft Windows 10 - Sandboxed Mount Reparse Point Creation Mitigation Bypass (MS15-[01;31m[K111[m[K) |
windows/local/38474.txt

Microsoft Windows 8.1 Update 2 / 10 10586 (x86/x64) - NtLoadKeyEx User Hive Attachment Point Privilege Esc | windows/local/40429.cs

Microsoft Windows Defender - ActiveX Heap Overflow (PoC)
| windows/dos/[01;31m[K111[m[K95.html

Microsoft Windows Explorer - '.WMF' CreateBrushIndirect Denial of Service |
windows/dos/3[01;31m[K111[m[K.pl

Microsoft Windows Messenger Service - Denial of Service (MS03-043)
| windows/dos/[01;31m[K111[m[K.c

Microsoft Windows NT/2000/2003/2008/XP/Vista/7 - 'KiTrap0D' User Mode to Ring Escalation (MS10-015) |
windows/local/[01;31m[K111[m[K99.txt

Microsoft Works 8.0 - File Converter Field Length Remote Code Execution
| windows/remote/3[01;31m[K111[m[K8.c

Millenium MP3 Studio 1.x - '.m3u' Local Stack Overflow
| windows/local/[01;31m[K111[m[K91.pl

Mini-stream Ripper 3.0.1.1 - '.smi' Local Buffer Overflow (PoC)
| windows/dos/[01;31m[K111[m[K97.py

MojoAuto - Blind SQL Injection
| cgi/webapps/6[01;31m[K111[m[K.pl

MoME CMS 0.8.5 - Remote Authentication Bypass
| php/webapps/[01;31m[K111[m[K57.txt

Moodle LMS 4.0 - Cross-Site Scripting (XSS)
| php/webapps/5[01;31m[K111[m[K5.txt

Multiple Media Players ((iTunes / QuickTime) - HTTP DataHandler Overflow |
multiple/dos/[01;31m[K111[m[K42.txt

```
Muziic Player 2.0 - '.mp3' Local Denial of Service
| windows/dos/[01;31m[K111[m[K80.pl

MyBloggie 2.1.x - 'index.php' Multiple SQL Injections
| php/webapps/30[01;31m[K111[m[K.txt

MyNews 1.6.x - 'hash' Cross-Site Scripting
| php/webapps/3[01;31m[K111[m[K5.txt

Nemesis Player (NSP) - Local Denial of Service
| windows/dos/[01;31m[K111[m[K32.pl

Netgear WG[01;31m[K111[m[Kv2 Wireless Driver - Long Beacon Overflow
(Metasploit)                                          |
hardware/remote/16388.rb

NPlayer - '.dat Skin' Local Heap Overflow (PoC)
| windows/dos/[01;31m[K111[m[K33.pl

Nuked KLan 1.7.7 & SP4 - Denial of Service
| multiple/dos/[01;31m[K111[m[K06.sh

Ofilter Player - 'skin.ini' Local Crash (PoC)
| windows/dos/[01;31m[K111[m[K30.pl

Online Tshirt Design Script - SQL Injection
| php/webapps/4[01;31m[K111[m[K0.txt

Open Bulletin Board 1.0.5 - SQL Injection
| php/webapps/[01;31m[K111[m[K1.pl

OpenGuestbook 0.5 - 'header.php?title' Cross-Site Scripting
| php/webapps/28[01;31m[K111[m[K.txt

OpenOffice - '.slk' Parsing Null Pointer
| windows/dos/[01;31m[K111[m[K92.txt

OPSWAT Metadefender Core - Privilege Escalation
| multiple/webapps/5[01;31m[K111[m[K3.py

OtsTurntables Free 1.00.047 - Overwrite (SEH) (PoC)
| windows/dos/[01;31m[K111[m[K45.pl

Pagetool 1.07 - 'search_term' Cross-Site Scripting
| php/webapps/3[01;31m[K111[m[K6.txt

PaNews 2.0 - Cross-Site Scripting
| php/webapps/25[01;31m[K111[m[K.txt

PHP-RESIDENCE 0.7.2 - Multiple Local File Inclusions
| php/webapps/[01;31m[K111[m[K56.txt
```

phpBB 2.0.15 - PHP Remote Code Execution (Metasploit)
| php/webapps/[01;31m[K111[m[K3.pm

PHPSiteBackup 0.1 - 'pcltar.lib.php' Remote File Inclusion
| php/webapps/4[01;31m[K111[m[K.txt

Pirelli DRG A115 v3 ADSL Router - DNS Change
| hardware/webapps/4[01;31m[K111[m[K8.sh

PonVFTP - Bypass / Arbitrary File Upload
| php/webapps/[01;31m[K111[m[K48.txt

Populum 2.3 - SQL Injection
| php/webapps/[01;31m[K111[m[K26.txt

Portail Web PHP 2.5.1 - 'login.php' Remote File Inclusion
| php/webapps/3[01;31m[K111[m[K0.txt

PostNuke 0.6 - User Login
| php/webapps/2[01;31m[K111[m[K9.txt

Pre Survey Generator - 'default.asp' SQL Injection
| asp/webapps/32[01;31m[K111[m[K.txt

Progress Database 8.3/9.1 - Multiple Buffer Overflows
| multiple/local/2[01;31m[K111[m[K7.txt

PSI CMS 0.3.1 - SQL Injection
| php/webapps/[01;31m[K111[m[K35.txt

Public Media Manager - SQL Injection
| php/webapps/[01;31m[K111[m[K36.txt

Quest Toad for Oracle Explain Plan Display ActiveX Control -
'QExplain2.dll 6.6.1.[01;31m[K111[m[K5' Remote File Creati |
windows/remote/18703.txt

Quick N Easy Web Server 3.3.8 - Denial of Service (PoC)
| windows/dos/48[01;31m[K111[m[K.py

RedHat Linux 7.0 Apache - Remote Username Enumeration
| linux/remote/2[01;31m[K111[m[K2.php

ReQlogic v11.3 - Reflected Cross-Site Scripting (XSS)
| aspx/webapps/5[01;31m[K111[m[K8.txt

RoseOnlineCMS 3 B1 - Remote Authentication Bypass
| php/webapps/[01;31m[K111[m[K58.txt

Rosoft Media Player 4.4.4 - Local Buffer Overflow (SEH) (1)
| windows/local/[01;31m[K111[m[K61.pl

```
ScriptsFeed (SF) Auto Classifieds Software - Arbitrary File Upload
| php/webapps/7[01;31m[K111[m[K.txt

Serva 2.0.0 - HTTP Server GET Remote Denial of Service
| windows/dos/24[01;31m[K111[m[K.py

Shiksha Educational Website Script - SQL Injection
| php/webapps/4[01;31m[K111[m[K1.txt

SkyPortal WebLinks 0.12 - Contents Change
| asp/webapps/8[01;31m[K111[m[K.txt

slickMsg - Cross-Site Scripting / HTML Injection
| php/webapps/35[01;31m[K111[m[K.txt

SlimFTPd 3.16 - Remote Buffer Overflow
| windows/remote/[01;31m[K111[m[K8.c

Social-Share-Buttons v2.2.3 - SQL Injection
| php/webapps/5[01;31m[K111[m[K6.txt

Soft Direct 1.05 - Multiple Vulnerabilities
| php/webapps/[01;31m[K111[m[K89.txt

SolarWinds TFTP Server 9.2.0.[01;31m[K111[m[K - Remote Denial of
Service                                                 |
windows/dos/9547.pl

Study Abroad Educational Website Script - SQL Injection
| php/webapps/4[01;31m[K111[m[K2.txt

Sub Station Alpha 4.08 - '.rt' Local Buffer Overflow (PoC)
| windows/dos/[01;31m[K111[m[K49.c

Subrion CMS 4.2.1 - Stored Cross-Site Scripting (XSS)
| php/webapps/5[01;31m[K111[m[K0.txt

Sungard eTRAKiT3 <= 3.2.1.17 - SQL Injection
| json/webapps/42[01;31m[K111[m[K.txt

SwiFTP 1.11 - Overflow (Denial of Service) (PoC)
| hardware/dos/[01;31m[K111[m[K25.pl

Tenda ADSL2/2+ Modem D820R - DNS Change
| hardware/webapps/4[01;31m[K111[m[K7.sh

Testlink TestManagement and Execution System 1.8.5 - Multiple Directory
Traversal Vulnerabilities          | php/webapps/[01;31m[K111[m[K83.txt

tincan ltd - 'section' SQL Injection
| php/webapps/[01;31m[K111[m[K13.txt
```

TinTin++ / WinTin++ 1.97.9 - '#chat' Multiple Vulnerabilities
| multiple/remote/3[01;31m[K111[m[K9.txt

TP-Link TD-8817 6.0.1 Build [01;31m[K111[m[K128 Rel.26763 - Cross-Site
Request Forgery |
hardware/webapps/24928.txt

TP-Link TL-WR740N [01;31m[K111[m[K130 - 'ping_addr' HTML Injection
| hardware/remote/36945.txt

Transload Script - Arbitrary File Upload
| php/webapps/[01;31m[K111[m[K55.txt

Trend Micro Email Encryption Gateway 5.5 (Build [01;31m[K111[m[K1.00) -
Multiple Vulnerabilities | jsp/webapps/44166.txt

Trend Micro Web-Deployment - ActiveX Remote Execution
| windows/remote/[01;31m[K111[m[K73.txt

Tunnel Interface Driver - Denial of Service
| windows/dos/5[01;31m[K111[m[K4.c

TurboFTP Server 1.00.712 - Remote Denial of Service
| windows/dos/[01;31m[K111[m[K31.pl

Uploader by CeleronDude 5.3.0 - Arbitrary File Upload (2)
| php/webapps/[01;31m[K111[m[K66.txt

VideoLAN VLC Media Player 0.8.6 a/b/c/d (Win32 Universal) - '.ass'
Local Buffer Overflow |
windows/local/[01;31m[K111[m[K74.c

VideoLAN VLC Media Player 0.8.6i - ActiveX Denial of Service (PoC)
| windows/dos/[01;31m[K111[m[K03.html

vim 6.3 < 6.3.082 - 'modlines' Local Command Execution
| multiple/local/[01;31m[K111[m[K9.txt

Viral Image & Video Sharing GagZone Script - SQL Injection
| php/webapps/4[01;31m[K111[m[K9.txt

Vite 6.2.2 - Arbitrary File Read
| multiple/remote/52[01;31m[K111[m[K.py

Winamp 5.05 < 5.13 - '.ini' Local Stack Buffer Overflow
| windows/local/[01;31m[K111[m[K39.c

WordPress Plugin MailChimp Subscribe Forms 1.1 - Remote Code Execution
| php/webapps/37[01;31m[K111[m[K.txt

WordPress Plugin Premium Gallery Manager - Arbitrary File Upload
| php/webapps/39[01;31m[K111[m[K.php

WordPress Plugin Simple Gmail Login - Stack Trace Information Disclosure | php/webapps/38[01;31m[K111[m[K.txt

WordPress Plugin Zingiri 2.2.3 - 'ajax_save_name.php' Remote Code Execution | php/webapps/18[01;31m[K111[m[K.php

X-Skipper-Proxy v0.13.237 - Server Side Request Forgery (SSRF) | multiple/remote/5[01;31m[K111[m[K1.txt

XMLBlueprint 16.19[01;31m[K111[m[K2 - XML External Entity Injection | windows/local/47974.txt

Xunlei XPPlayer 5.9.14.1246 - ActiveX Remote Execution (PoC) | windows/dos/[01;31m[K111[m[K76.txt

Yaws-Wiki 1.88-1 (Erlang) - Persistent / Reflective Cross-Site Scripting | multiple/webapps/17[01;31m[K111[m[K.txt

ZKTeco ZEM/ZMM 8.88 - Missing Authentication | jsp/webapps/5[01;31m[K111[m[K2.txt

---

Shellcode Title | Path

FreeBSD/x86 - Bind (31337/TCP) Shell (/bin/sh) + fork() Shellcode ([01;31m[K111[m[K bytes) | freebsd_x86/16026.c

Linux/x86 - Bind ([01;31m[K111[m[K1/TCP) Shell + GetPC/Call/Ret Method + Null-Free Shellcode (89 bytes) | linux_x86/43729.c

Linux/x86 - Bind ([01;31m[K111[m[K1/TCP) Shell + Null-Free Shellcode (73 bytes) | linux_x86/43730.c

Linux/x86 - Bind ([01;31m[K111[m[K1/TCP) Shell + SO_REUSEADDR Set (Avoiding SIGSEGV) + Null-Free Shellcode (103 bytes) | linux_x86/43726.c

Linux/x86 - Download File (HTTP/1.x http://0xdeadbeef/A) + execve() + Null-Free Shellcode ([01;31m[K111[m[K+ bytes) | linux_x86/13355.c

Linux/x86 - Reverse (127.1.1.1:[01;31m[K111[m[K11/TCP) Shell + Null-Free Shellcode (67 bytes) | linux_x86/42295.c

Linux/x86 - Reverse (127.1.1.1:12345/TCP) cat /etc/passwd Shellcode ([01;31m[K111[m[K bytes) | linux_x86/43747.c

Windows/x86 - Add Administrator User (GAZZA/123456) + Start Telnet Service Shellcode ([01;31m[K111[m[K bytes) | windows_x86/13508.asm

---

Port: 135

Exploit Title | Path

2^6 TCP Control Bit - Fuzzer (No ECN or CWR) | multiple/remote/[01;31m[K135[m[K88.pl

Adobe Flash Player 11.5.502.[01;31m[K135[m[K - Crash (PoC) | windows/dos/23469.txt

Apache Struts 2 - DefaultActionMapper Prefixes OGNL Code Execution (Metasploit) | multiple/remote/27[01;31m[K135[m[K.rb

Apache Win32 1.3.x/2.0.x - Batch File Remote Command Execution | windows/remote/2[01;31m[K135[m[K0.pl

Apple Mac OSX 10.4.x - OpenLDAP Denial of Service | osx/dos/28[01;31m[K135[m[K.pl

ASUS DSL-N12E_C1 1.1.2.3_345 - Remote Command Execution | hardware/webapps/45[01;31m[K135[m[K.txt

Avast! 4.8.[01;31m[K135[m[K1.0 AntiVirus - 'aswMon2.sys' Kernel Memory Corruption | windows/dos/10106.c

Avast! AntiVirus 4.8.[01;31m[K135[m[K1.0 - Denial of Service / Privilege Escalation | windows/local/9831.txt

Avast! AntiVirus 4.8.[01;31m[K135[m[K6 - 'aswRdr.sys' Driver Privilege Escalation |
windows/local/33360.c

Belkatalog CMS - SQL Injection
| php/webapps/1[01;31m[K135[m[K0.txt

BrainyCP V1.0 - Remote Code Execution
| php/webapps/5[01;31m[K135[m[K7.py

Car Portal 2.0 - Blind SQL Injection
| php/webapps/15[01;31m[K135[m[K.txt

CDBurnerXP 4.2.4.[01;31m[K135[m[K1 - Local Crash (Denial of Service)
| windows/dos/9814.py

CiMe Citas Médicas - Multiple Vulnerabilities
| php/webapps/3[01;31m[K135[m[K0.txt

Citrix NFuse 1.51/1.6 - Cross-Site Scripting
| jsp/remote/2[01;31m[K135[m[K5.txt

ClicShopping v3.402 - Cross-Site Scripting (XSS)
| php/webapps/51[01;31m[K135[m[K.txt

common Solutions csphonebook 1.02 - 'index.php' Cross-Site Scripting
| php/webapps/32[01;31m[K135[m[K.txt

Croogo 1.2.1 - Multiple Cross-Site Request Forgery Vulnerabilities
| php/webapps/1[01;31m[K135[m[K3.txt

CSSearch 2.3 - Remote Command Execution
| cgi/remote/2[01;31m[K135[m[K4.txt

DCShop Beta 1.0 - Form Manipulation
| cgi/webapps/2[01;31m[K135[m[K2.txt

DjVuLibre 3.5.25.3 - Out of Bounds Access Violation
| windows/dos/34[01;31m[K135[m[K.py

DoceboLms 2.0.4 - 'connector.php' Arbitrary File Upload
| php/webapps/[01;31m[K135[m[K6.php

dotclear 2.25.3 - Remote Code Execution (RCE) (Authenticated)
| php/webapps/5[01;31m[K135[m[K3.txt

dotProject 2.1.5 - Cross-Site Request Forgery
| php/webapps/16[01;31m[K135[m[K.html

EncapsCMS 0.3.6 - 'config[path]' Remote File Inclusion
| php/webapps/1[01;31m[K135[m[K5.txt

```
ESET Service 16.0.26.0 - 'Service ekrn' Unquoted Service Path
| windows/local/5[01;31m[K135[m[K1.txt

ever gauzy v0.281.9 - JWT weak HMAC secret
| typescript/webapps/5[01;31m[K135[m[K4.txt

FipsCMS Light 2.1 - 'r' SQL Injection
| asp/webapps/6[01;31m[K135[m[K.txt

FireFly Mediaserver 1.0.0.[01;31m[K135[m[K9 - Null Pointer Dereference
| windows/dos/23574.txt

FloosieTek FTGatePro 1.2 - WebAdmin Interface Information Disclosure
| windows/remote/23[01;31m[K135[m[K.txt

Google Android - android.util.MemoryIntArray Ashmem Race Conditions
| android/dos/4[01;31m[K135[m[K5.txt

Google Android - Inter-process munmap in android.util.MemoryIntArray
| android/dos/4[01;31m[K135[m[K4.txt

iGuard Security Access Control Device Firmware 3.6.7427A - Cross-Site
Scripting                              |
hardware/webapps/37[01;31m[K135[m[K.txt

ImageVue 1.7 - 'dir2.php?path' Cross-Site Scripting
| php/webapps/3[01;31m[K135[m[K3.txt

ImageVue 1.7 - 'dirxml.php?path' Cross-Site Scripting
| php/webapps/3[01;31m[K135[m[K5.txt

ImageVue 1.7 - 'popup.php?path' Cross-Site Scripting
| php/webapps/3[01;31m[K135[m[K2.txt

ImageVue 1.7 - 'upload.php?path' Cross-Site Scripting
| php/webapps/3[01;31m[K135[m[K4.txt

Itech B2B Script 4.29 - Multiple Vulnerabilities
| php/webapps/4[01;31m[K135[m[K9.txt

Java Applet - Driver Manager Privileged 'toString()' Remote Code
Execution (Metasploit)                 |
multiple/remote/26[01;31m[K135[m[K.rb

JaxCMS 1.0 - Local File Inclusion
| php/webapps/1[01;31m[K135[m[K9.txt

Joomla! Component Classified - SQL Injection
| php/webapps/35[01;31m[K135[m[K.txt

Joomla! Component com_bit - 'Controller' Local File Inclusion
| php/webapps/38[01;31m[K135[m[K.txt
```

```
Joomla! Component com_productbook - SQL Injection
| php/webapps/1[01;31m[K135[m[K2.txt

Joomla! Component SquadManagement 1.0.3 - SQL Injection
| php/webapps/44[01;31m[K135[m[K.txt

KEMP LoadMaster 7.[01;31m[K135[m[K.0.13245 - Persistent Cross-Site
Scripting / Remote Code Execution                    |
multiple/webapps/42090.txt

Killmonster 2.1 - Authentication Bypass
| php/webapps/1[01;31m[K135[m[K4.txt

LG G4 - lgdrmserver Binder Service Multiple Race Conditions
| android/dos/4[01;31m[K135[m[K1.txt

LG G4 - lghashstorageserver Directory Traversal
| android/dos/4[01;31m[K135[m[K2.txt

LG G4 - Touchscreen Driver write_log Kernel Read/Write
| android/dos/4[01;31m[K135[m[K3.txt

Linux Kernel - 'ping' Local Denial of Service
| android/dos/42[01;31m[K135[m[K.c

Linux Kernel 2.2.x/2.3/2.4.x - 'd_path()' Path Truncation
| linux/local/2[01;31m[K135[m[K3.c

Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation
| linux/local/50[01;31m[K135[m[K.c

Linux Kernel 3.10.0 (CentOS 7) - Denial of Service
| linux/dos/4[01;31m[K135[m[K0.c

LogWatch 2.1.1/2.5 - Insecure Temporary Directory Creation
| linux/local/2[01;31m[K135[m[K6.sh

Magento WooCommerce CardGate Payment Gateway 2.0.30 - Payment Process
Bypass                                |
php/webapps/48[01;31m[K135[m[K.php

Media Commands - '.m3u' / '.m3l' / '.TXT' / '.LRC' Local Heap Overflow
(PoC)                                 | windows/dos/8[01;31m[K135[m[K.pl

Microsoft Edge (Chromium-based) Webview2 1.0.1661.34 - Spoofing
| multiple/local/5[01;31m[K135[m[K9.txt

Microsoft Edge - TypedArray.sort Use-After-Free (MS16-145)
| windows/dos/4[01;31m[K135[m[K7.html

Microsoft Internet Explorer 5.0.1 - CSS Style Sheet Memory Corruption
| windows/dos/24[01;31m[K135[m[K.html
```

```
Microsoft Internet Explorer 7 - Combined JavaScript and XML Remote
Information Disclosure                  |
windows/remote/3[01;31m[K135[m[K9.html

Microsoft Windows - DTC Remote (MS05-051) (2)
| windows/remote/[01;31m[K135[m[K2.cpp

Microsoft Windows 10 1903/1809 - RPCSS Activation Kernel Security
Callback Privilege Escalation           |
windows/local/47[01;31m[K135[m[K.txt

Microsoft Windows Kernel - 'win32k' Denial of Service (MS16-
[01;31m[K135[m[K                                                |
windows/dos/40745.c

Microsoft Windows Kernel - 'win32k.sys NtSetWindowLongPtr' Local
Privilege Escalation (MS16-[01;31m[K135[m[K) (1)       |
windows/local/40823.txt

Microsoft Windows Kernel - 'win32k.sys NtSetWindowLongPtr' Local
Privilege Escalation (MS16-[01;31m[K135[m[K) (2)       |
windows/local/41015.c

Microsoft Windows Messenger Service (French) - Remote (MS03-043)
| windows/remote/[01;31m[K135[m[K.c

Mini Blog 1.1 - Authentication Bypass
| php/webapps/41[01;31m[K135[m[K.txt

Multi Restaurant Table Reservation System 1.0 - Multiple Persistent XSS
| php/webapps/49[01;31m[K135[m[K.txt

mygamingladder MGL Combo System 7.5 - SQL Injection
| php/webapps/12[01;31m[K135[m[K.txt

nai net tools pki server 1.0 - Directory Traversal
| windows/remote/20[01;31m[K135[m[K.txt

NEWSolved Lite 1.9.2 - 'abs_path' Remote File Inclusion
| php/webapps/2[01;31m[K135[m[K.txt

ntfs-3g - Unsanitized modprobe Environment Privilege Escalation
| linux/local/4[01;31m[K135[m[K6.txt

Okul Web Otomasyon Sistemi 4.0.1 - SQL Injection
| asp/webapps/3[01;31m[K135[m[K.txt

Online Computer and Laptop Store 1.0 - Remote Code Execution (RCE)
| php/webapps/5[01;31m[K135[m[K8.py

Openswan 2.4.12/2.6.16 - Insecure Temp File Creation Privilege
Escalation                              |
linux/local/9[01;31m[K135[m[K.sh
```

```
Opera 9.62 - 'file://' Local Heap Overflow
| windows/local/7[01;31m[K135[m[K.html

Paradox Security Systems IPR512 - Denial Of Service
| hardware/dos/5[01;31m[K135[m[K6.sh

Pentaho BA Server EE 9.3.0.0-428 - Remote Code Execution (RCE)
(Unauthenticated)                              |
jsp/webapps/5[01;31m[K135[m[K0.txt

pfsenseCE v2.6.0 - Anti-brute force protection bypass
| hardware/remote/5[01;31m[K135[m[K2.py

PHP-Fusion 6.0.106 - BBCode IMG Tag Script Injection
| php/webapps/1[01;31m[K135[m[K.c

PHP-Nuke 4nChat Module 0.91 - 'roomid' SQL Injection
| php/webapps/3[01;31m[K135[m[K1.txt

phpEventCalendar 0.2.3 - 'eventdisplay.php' SQL Injection
| php/webapps/4[01;31m[K135[m[K.pl

PHPLive! 3.2.2 - '/admin/header.php?admin[name]' Cross-Site Scripting
| php/webapps/30[01;31m[K135[m[K.txt

Piwik [01;31m[K135[m[K7 2009-08-02 - Arbitrary File Upload / Code
Execution                                                  |
php/webapps/9962.txt

Piwik 2.14.0/2.16.0/2.17.1/3.0.1 - Superuser Plugin Upload (Metasploit)
| php/remote/4[01;31m[K135[m[K8.rb

PostNuke 0.703 - caselist Arbitrary Module Include
| php/webapps/2[01;31m[K135[m[K7.txt

Progress Database 9.1 - sqlcpp Local Buffer Overflow
| multiple/local/2[01;31m[K135[m[K9.c

PSI CMS 0.3.1 - SQL Injection
| php/webapps/11[01;31m[K135[m[K.txt

Rapid Classified 3.1 - 'search.asp' Cross-Site Scripting
| asp/webapps/29[01;31m[K135[m[K.txt

Rapid-Source Rapid-Recipe Component - Multiple SQL Injections
| php/webapps/31[01;31m[K135[m[K.txt

Rostermain 1.1 - Authentication Bypass
| php/webapps/1[01;31m[K135[m[K6.txt

Roxy Fileman 1.4.5 -  Arbitrary File Upload
| ashx/webapps/5[01;31m[K135[m[K5.txt
```

Rumble Mail Server 0.51.3[01;31m[K135[m[K - 'domain and path' Stored XSS | multiple/webapps/49254.txt

Rumble Mail Server 0.51.3[01;31m[K135[m[K - 'rumble_win32.exe' Unquoted Service Path | windows/local/49203.txt

Rumble Mail Server 0.51.3[01;31m[K135[m[K - 'servername' Stored XSS | multiple/webapps/49253.txt

Rumble Mail Server 0.51.3[01;31m[K135[m[K - 'username' Stored XSS | multiple/webapps/49255.txt

SimpleBBS 1.1 - Remote Command Execution | php/webapps/[01;31m[K135[m[K8.php

sobexsrv 1.0.0_pre3 Bluetooth - 'syslog()' Remote Format String | linux/remote/[01;31m[K135[m[K5.pl

Solaris/Open Solaris UCODE_GET_VERSION IOCTL - Denial of Service | solaris/dos/1[01;31m[K135[m[K1.c

Specimen Image Database - 'taxonservice.php?dir' Remote File Inclusion | php/webapps/3[01;31m[K135[m[K8.txt

Squirrelcart Cart Shop 3.3.4 - Multiple Web Vulnerabilities | php/webapps/19[01;31m[K135[m[K.txt

SquirrelMail 1.2.x - Theme Remote Command Execution | php/webapps/2[01;31m[K135[m[K8.sh

SugarSuite Open Source 4.0beta - Remote Code Execution (1) | php/webapps/[01;31m[K135[m[K9.php

Syslog Watcher Pro 2.8.0.812 - 'Date' Cross-Site Scripting | windows/dos/25[01;31m[K135[m[K.txt

TANne 0.6.17 - Session Manager SysLog Format String | linux/remote/22[01;31m[K135[m[K.c

TestLink 1.9.3 - Cross-Site Request Forgery | php/webapps/21[01;31m[K135[m[K.txt

TinyMCE WYSIWYG Editor - Multiple Vulnerabilities | php/webapps/1[01;31m[K135[m[K8.txt

Uiga Business Portal - SQL Injection / Cross-Site Scripting | php/webapps/1[01;31m[K135[m[K7.txt

viscacha 0.8.1 - Multiple Vulnerabilities | php/webapps/17[01;31m[K135[m[K.txt

```
WIDCOMM Bluetooth Software < 3.0 - Remote Buffer Overflow
| windows/remote/[01;31m[K135[m[K7.diff

WinEggDropShell 1.7 - Multiple Remote Stack Overflows (PoC)
| windows/dos/[01;31m[K135[m[K3.py

WordPress Core 2.3.2 - '/wp-admin/invites.php?to' Cross-Site Scripting
| php/webapps/3[01;31m[K135[m[K7.txt

WordPress Core 2.3.2 - '/wp-admin/users.php?inviteemail' Cross-Site
Scripting                                |
php/webapps/3[01;31m[K135[m[K6.txt

WordPress Plugin Auctions 1.8.8 - 'wpa_id' SQL Injection
| php/webapps/36[01;31m[K135[m[K.txt

WordPress Plugin Photo album - SQL Injection
| php/webapps/5[01;31m[K135[m[K.txt

WordPress Theme Felici - 'Uploadify.php' Arbitrary File Upload
| php/webapps/39[01;31m[K135[m[K.php

WorkforceROI Xpede 4.1/7.0 - Weak Password Encryption
| windows/local/2[01;31m[K135[m[K1.pl

Wowza Streaming Engine 4.5.0 - Multiple Cross-Site Scripting
Vulnerabilities                          |
multiple/webapps/40[01;31m[K135[m[K.txt

Xlight FTP Server 3.8.8.5 - Buffer Overflow (PoC)
| windows/dos/43[01;31m[K135[m[K.py

YesWiki 4.5.1 - Unauthenticated Path Traversal
| multiple/webapps/52[01;31m[K135[m[K.txt

Zen Cart 1.2.6d - 'password_forgotten.php' SQL Injection
| php/webapps/[01;31m[K135[m[K4.php

---------------------------------------------------------------------------------------- ----------
----------

---------------------------------------------------------------------------------------- ----------
----------
Shellcode Title
|  Path

---------------------------------------------------------------------------------------- ----------
----------
FreeBSD/x86 - Bind (1337/TCP) Shell (/bin/sh) Shellcode (167 bytes)
| freebsd_x86/[01;31m[K135[m[K70.c
```

Linux/x64 - Reverse (127.0.0.1:4444/TCP) Shell + Password (hack) + Polymorphic Shellcode ([01;31m[K135[m[K bytes) | linux_x86-64/39388.c

Linux/x86 - Add Root User (toor) To /etc/passwd + No Password + exit() Shellcode (107 bytes) | linux_x86/[01;31m[K135[m[K79.c

Linux/x86 - chmod 0666 /etc/shadow + exit() Shellcode (33 bytes) | linux_x86/[01;31m[K135[m[K51.c

Linux/x86 - chmod 666 /etc/shadow Shellcode (27 bytes) | linux_x86/[01;31m[K135[m[K76.asm

Linux/x86 - Download File + Execute Shellcode ([01;31m[K135[m[K bytes) | linux_x86/39389.c

Linux/x86 - Eject /dev/cdrom Shellcode (42 bytes) | linux_x86/[01;31m[K135[m[K86.asm

Linux/x86 - execve() Shellcode (51 bytes) | linux_x86/[01;31m[K135[m[K53.c

Linux/x86 - Fork Bomb Shellcode (6 bytes) (1) | linux_x86/[01;31m[K135[m[K78.asm

Linux/x86 - ip6tables -F + Polymorphic Shellcode (71 bytes) | linux_x86/[01;31m[K135[m[K99.c

Linux/x86 - Kill All Processes Shellcode (9 bytes) | linux_x86/[01;31m[K135[m[K48.asm

Linux/x86 - Overwrite MBR On /dev/sda With _LOL!' Shellcode (43 bytes) | linux_x86/[01;31m[K135[m[K63.asm

Linux/x86 - setreuid(0_0) + execve(/bin/rm /etc/shadow) Shellcode | linux_x86/[01;31m[K135[m[K66.c

Linux/x86 - setuid() + Break chroot (mkdir/chdir/chroot '...') + execve(/bin/sh) Shellcode (79 bytes) | linux_x86/[01;31m[K135[m[K77.txt

Linux/x86 - setuid(0) + /bin/cat /etc/shadow Shellcode (49 bytes) | linux_x86/[01;31m[K135[m[K50.c

Linux/x86 - setuid(0) + execve(/sbin/poweroff -f) Shellcode (47 bytes) | linux_x86/[01;31m[K135[m[K49.c

Linux/x86 - unlink(/etc/passwd) + exit() Shellcode (35 bytes) | linux_x86/[01;31m[K135[m[K72.c

Solaris/x86 - execve(/bin/sh) ToUpper Encoded Shellcode (84 bytes) | solaris_x86/[01;31m[K135[m[K01.c

Solaris/x86 - inetd Add Service + execve() Shellcode (201 bytes)
| solaris_x86/[01;31m[K135[m[K02.c

Solaris/x86 - setuid(0) + execve(/bin/cat_ /etc/shadow) + exit(0)
Shellcode (59 bytes) |
solaris_x86/[01;31m[K135[m[K00.c

UnixWare - execve(/bin/sh) Shellcode (95 bytes)
| unixware/[01;31m[K135[m[K03.c

Windows (9x/NT/2000/XP) - PEB Method Shellcode (29 bytes)
| windows_x86/[01;31m[K135[m[K25.c

Windows (9x/NT/2000/XP) - PEB Method Shellcode (31 bytes)
| windows_x86/[01;31m[K135[m[K26.c

Windows (9x/NT/2000/XP) - PEB Method Shellcode (35 bytes)
| windows_x86/[01;31m[K135[m[K27.c

Windows (9x/NT/2000/XP) - Reverse Generic Without Loader
(192.168.1.11:4919) Shellcode (249 bytes) |
windows_x86/[01;31m[K135[m[K24.txt

Windows (NT/2000/XP) (Russian) - Add Administartor User (slim/shady)
Shellcode (318 bytes) |
windows_x86/[01;31m[K135[m[K23.c

Windows (XP Professional SP2) (English) - MessageBox + Null-Free
Shellcode (16 bytes) |
windows/[01;31m[K135[m[K81.txt

Windows (XP Professional SP2) (English) - Wordpad.exe + Null-Free
Shellcode (12 bytes) |
windows/[01;31m[K135[m[K82.txt

Windows (XP SP1) - Bind (58821/TCP) Shell Shellcode (116 bytes)
| windows_x86/[01;31m[K135[m[K31.c

Windows (XP SP2) - PEB ISbeingdebugged Beep Shellcode (56 bytes)
| windows/[01;31m[K135[m[K60.txt

Windows (XP) - Download File (http://www.elitehaven.net/ncat.exe) +
Execute (nc.exe) + Null-Free Shellcode |
windows_x86/[01;31m[K135[m[K30.asm

Windows (XP/2000/2003) - Download File (http://127.0.0.1/test.exe) +
Execute (%systemdir%/a.exe) Shellcode |
windows_x86/[01;31m[K135[m[K29.c

Windows (XP/2000/2003) - Reverse (127.0.0.1:53/TCP) Shell Shellcode
(275 bytes) (Generator) | generator/[01;31m[K135[m[K28.c

```
Windows - DCOM RPC2 Universal Shellcode
| windows_x86/[01;31m[K135[m[K32.asm

Windows/x64 - URLDownloadToFileA(http://localhost/trojan.exe) + Execute
Shellcode (218+ bytes)             | windows_x86-
64/[01;31m[K135[m[K33.asm

Windows/x86 (5.0 < 7.0) - Bind (28876/TCP) Shell + Null-Free Shellcode
| windows_x86/[01;31m[K135[m[K04.asm

Windows/x86 (NT/XP) - IsDebuggerPresent Shellcode (39 bytes)
| windows_x86/[01;31m[K135[m[K18.c

Windows/x86 (SP1/SP2) - Beep Shellcode (35 bytes)
| windows_x86/[01;31m[K135[m[K19.c

Windows/x86 (XP SP2) (English / Arabic) - cmd.exe Shellcode (23 bytes)
| windows_x86/[01;31m[K135[m[K74.c

Windows/x86 (XP SP2) (English) - cmd.exe Shellcode (23 bytes)
| windows_x86/[01;31m[K135[m[K05.c

Windows/x86 (XP SP2) (French) - calc.exe Shellcode (19 bytes)
| windows_x86/[01;31m[K135[m[K95.c

Windows/x86 (XP SP2) (French) - cmd.exe Shellcode (32 bytes)
| windows_x86/[01;31m[K135[m[K10.c

Windows/x86 (XP SP2) - calc.exe Shellcode (45 bytes)
| windows_x86/[01;31m[K135[m[K71.c

Windows/x86 (XP SP2) - cmd.exe Shellcode (57 bytes)
| windows_x86/[01;31m[K135[m[K11.c

Windows/x86 (XP SP2) - MessageBox Shellcode (110 bytes)
| windows_x86/[01;31m[K135[m[K20.c

Windows/x86 (XP SP3) - Add Firewall Rule (Allow 445/TCP) Shellcode
| windows_x86/[01;31m[K135[m[K69.asm

Windows/x86 (XP SP3) - ShellExecuteA() Shellcode
| windows_x86/[01;31m[K135[m[K65.asm

Windows/x86 - Add Administrator User (GAZZA/123456) + Start Telnet
Service Shellcode (111 bytes)          |
windows_x86/[01;31m[K135[m[K08.asm

Windows/x86 - Command WinExec() Shellcode (104+ bytes)
| windows_x86/[01;31m[K135[m[K21.asm

Windows/x86 - Download File (http://127.0.0.1/file.exe) + Execute
Shellcode (124 bytes)                   |
windows_x86/[01;31m[K135[m[K17.asm
```

Windows/x86 - Download File (http://www.ph4nt0m.org/a.exe) + Execute (C:/a.exe) Shellcode (226+ bytes) | windows_x86/[01;31m[K135[m[K22.c

Windows/x86 - Download File + Execute Shellcode (192 bytes) | windows_x86/[01;31m[K135[m[K16.asm

Windows/x86 - Download File + Execute Shellcode (Browsers Edition) (275+ bytes) (Generator) | generator/[01;31m[K135[m[K15.pl

Windows/x86 - Egg Omelet SEH Shellcode | windows_x86/[01;31m[K135[m[K07.txt

Windows/x86 - PEB 'Kernel32.dll' ImageBase Finder + Alphanumeric Shellcode (67 bytes) | windows_x86/[01;31m[K135[m[K12.c

Windows/x86 - PEB 'Kernel32.dll' ImageBase Finder + ASCII Printable Shellcode (49 bytes) | windows_x86/[01;31m[K135[m[K13.c

Windows/x86 - PEB!NtGlobalFlags Shellcode (14 bytes) | windows_x86/[01;31m[K135[m[K09.c

Windows/x86 - Reverse (/TCP) + Download File + Save + Execute Shellcode | windows_x86/[01;31m[K135[m[K14.asm

---

Port: 139

Exploit Title | Path

(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Full System Access | windows/remote/[01;31m[K139[m[K32.py

(Gabriel's FTP Server) Open & Compact FTPd 1.2 - Crash (PoC) | windows/dos/1[01;31m[K139[m[K1.py

ActiveFax (ActFax) 4.3 - Client Importer Buffer Overflow (Metasploit) | windows/local/21[01;31m[K139[m[K.rb

```
Adobe Illustrator CS5.5 - Memory Corruption
| multiple/local/19[01;31m[K139[m[K.py

Agnitum Outpost Firewall 4.0 - Outpost_IPC_HDR Local Denial of Service
| multiple/dos/30[01;31m[K139[m[K.c

Alpin CMS - 'e4700.asp?id' SQL Injection
| php/webapps/[01;31m[K139[m[K82.txt

Alpin CMS 1.0 - SQL Injection
| php/webapps/[01;31m[K139[m[K61.txt

Ananda Image Gallery - SQL Injection
| asp/webapps/[01;31m[K139[m[K02.txt

Arcsoft PhotoStudio 6.0.0.172 - Unquoted Service Path
| windows/local/5[01;31m[K139[m[K3.txt

Artifex MuPDF mujstest 1.10a - Null Pointer Dereference
| linux/dos/42[01;31m[K139[m[K.txt

AtomatiCMS - Upload Arbitrary File
| asp/webapps/15[01;31m[K139[m[K.txt

Auto Database System 1.0 Infusion Addon - SQL Injection
| php/webapps/16[01;31m[K139[m[K.txt

Ay Computer (Multiple Products) - Multiple SQL Injections
| asp/webapps/36[01;31m[K139[m[K.txt

Banner Management Script - SQL Injection
| php/webapps/[01;31m[K139[m[K29.txt

Batch Audio Converter Lite Edition 1.0.0.0 - Local Stack Buffer
Overflow (SEH)                                |
windows/local/[01;31m[K139[m[K09.py

BlazeDVD 5.1 (Windows 7) - '.plf' File Stack Buffer Overflow (ASLR +
DEP Bypass)                                |
windows/local/[01;31m[K139[m[K05.py

BlazeDVD 6.0 - '.plf' File Universal Buffer Overflow (SEH)
| windows/local/[01;31m[K139[m[K98.pl

Boa Web Server v0.94.14 - Authentication Bypass
| linux/webapps/51[01;31m[K139[m[K.txt

Boat Classifieds - 'printdetail.asp?Id' SQL Injection
| asp/webapps/[01;31m[K139[m[K95.txt

Boat Classifieds - SQL Injection
| asp/webapps/[01;31m[K139[m[K90.txt
```

```
BZFlag 2.0.4 - undelimited string Denial of Service
| multiple/dos/[01;31m[K139[m[K0.c

Chris LaPointe Download Center 1.2 - 'category' Cross-Site Scripting
| php/webapps/3[01;31m[K139[m[K0.txt

Chris LaPointe Download Center 1.2 - 'search' Cross-Site Scripting
| php/webapps/3[01;31m[K139[m[K1.txt

Cisco User-Changeable Password (UCP) 3.3.4.12.5 - 'CSUserCGI.exe' Help
Facility Cross-Site Scripting       |
windows/remote/3[01;31m[K139[m[K5.txt

Cisco User-Changeable Password (UCP) 3.3.4.12.5 - 'CSuserCGI.exe'
Multiple Remote Vulnerabilities          |
windows/dos/3[01;31m[K139[m[K4.txt

Classifieds Script - 'rate' SQL Injection
| php/webapps/[01;31m[K139[m[K71.txt

Colloquy 2.1.3545 - 'INVITE' Format String Denial of Service
| osx/dos/3[01;31m[K139[m[K.rb

Corel VideoStudio Pro X3 - '.mp4' Buffer Overflow
| windows/dos/[01;31m[K139[m[K19.c

Cornerstone CMS - SQL Injection
| php/webapps/[01;31m[K139[m[K80.txt

CubeCart 3.0.6 - Remote Command Execution
| php/webapps/[01;31m[K139[m[K8.pl

Cyrus IMSPD 1.7 - 'abook_dbname' Remote Code Execution
| linux/remote/[01;31m[K139[m[K.c

Easy Travel Portal - SQL Injection
| php/webapps/[01;31m[K139[m[K00.txt

Elite Gaming Ladders 3.5 - 'ladder[id]' SQL Injection
| php/webapps/[01;31m[K139[m[K36.txt

EPShop < 3.0 - 'pid' SQL Injection
| php/webapps/6[01;31m[K139[m[K.txt

Ethereal 10.x - AFP Protocol Dissector Remote Format String
| linux/remote/1[01;31m[K139[m[K.c

ezb systems ultraiso 8.0.[01;31m[K139[m[K2 - Directory Traversal
| windows/remote/27758.txt

File Sharing Wizard 1.5.0 - Remote Overflow (SEH)
| windows/remote/[01;31m[K139[m[K03.py
```

```
Fortigate UTM WAF Appliance - Multiple Vulnerabilities
| hardware/webapps/2[01;31m[K139[m[K5.txt

freeForum 1.7 - 'acuparam' Cross-Site Scripting
| php/webapps/32[01;31m[K139[m[K.txt

G.CMS Generator - SQL Injection
| php/webapps/[01;31m[K139[m[K54.txt

Gaim AIM/ICQ Protocols - Multiple Vulnerabilities
| windows/dos/26[01;31m[K139[m[K.txt

GameRoom Script - Authentication Bypass / Arbitrary File Upload
| php/webapps/1[01;31m[K139[m[K8.txt

Greeting card 1.1 - SQL Injection
| php/webapps/[01;31m[K139[m[K83.txt

H264WebCam - Boundary Condition Error
| windows/dos/[01;31m[K139[m[K20.c

Hacker Evolution Game: untold Mod Editor 2.00.001 - Buffer Overflow
(PoC)                                    |
windows/dos/[01;31m[K139[m[K39.pl

Half-Life ClanMod 1.80/1.81 Plugin - Remote Format String
| multiple/remote/22[01;31m[K139[m[K.c

Havij 1.10 - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K139[m[K12.txt

Home FTP Server 1.10.1.[01;31m[K139[m[K - 'SITE INDEX' Remote Denial of
Service                                          | windows/dos/9852.py

Hot or Not Picture Rating Script - SQL Injection
| php/webapps/[01;31m[K139[m[K73.txt

iBoutique - 'page' SQL Injection / Cross-Site Scripting
| php/webapps/[01;31m[K139[m[K45.txt

IcrediBB 1.1 - Script Injection
| php/webapps/2[01;31m[K139[m[K9.txt

IKARUS anti.virus 2.16.7 - 'ntguard_x64' Local Privilege Escalation
| windows_x86-64/local/43[01;31m[K139[m[K.c

Intel(R) Management Engine Components 8.0.1.[01;31m[K139[m[K9 -
Unquoted Service Path Privilege Escalation              |
windows/local/40579.txt

Jeebles Directory 2.9.60 - Multiple Cross-Site Scripting
Vulnerabilities                                    |
php/webapps/3[01;31m[K139[m[K3.txt
```

JetAudio 7.5.3 COWON Media Center - '.wav' Crash
| windows/dos/9[01;31m[K139[m[K.pl

JibberBook 2.3 - 'Login_form.php' Authentication Bypass
| php/webapps/37[01;31m[K139[m[K.txt

Job Search Engine Script - SQL Injection
| php/webapps/[01;31m[K139[m[K78.txt

Job Search Script - SQL Injection
| php/webapps/[01;31m[K139[m[K69.txt

Joomla! Component Answers 2.3beta - Multiple Vulnerabilities
| php/webapps/[01;31m[K139[m[K23.txt

Joomla! Component Bazaar Platform 3.0 - SQL Injection
| php/webapps/4[01;31m[K139[m[K0.txt

Joomla! Component com_community - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K139[m[K55.txt

Joomla! Component com_eportfolio - Arbitrary File Upload
| php/webapps/[01;31m[K139[m[K51.txt

Joomla! Component com_jomestate - Remote File Inclusion
| php/webapps/[01;31m[K139[m[K56.txt

Joomla! Component com_joomdocs - Cross-Site Scripting
| php/webapps/[01;31m[K139[m[K22.txt

Joomla! Component com_listbingo 1.3 - Multiple Vulnerabilities
| php/webapps/[01;31m[K139[m[K26.txt

Joomla! Component com_ybggal 1.0 - 'catid' SQL Injection
| php/webapps/[01;31m[K139[m[K79.txt

Joomla! Component Google Map Store Locator 4.4 - SQL Injection
| php/webapps/4[01;31m[K139[m[K1.txt

Joomla! Component JE Ajax Event Calendar 1.0.5 - SQL Injection
| php/webapps/[01;31m[K139[m[K97.txt

Joomla! Component JomSocial 1.6.288 - Multiple Cross-Site Scripting
Vulnerabilities |
php/webapps/[01;31m[K139[m[K62.txt

Joomla! Component MaQma Helpdesk 4.2.7 - 'id' SQL Injection
| php/webapps/4[01;31m[K139[m[K9.txt

Joomla! Component Most Wanted Real Estate 1.1.0 - SQL Injection
| php/webapps/4[01;31m[K139[m[K3.txt

Joomla! Component Ozio Gallery 2 - Multiple Vulnerabilities
| php/webapps/[01;31m[K139[m[K25.txt

Joomla! Component Picasa2Gallery 1.2.8 - Local File Inclusion
| php/webapps/[01;31m[K139[m[K81.txt

Joomla! Component RSComments 1.0.0 - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K139[m[K35.txt

jspwiki 2.4.104/2.5.[01;31m[K139[m[K - Multiple Vulnerabilities
| jsp/webapps/5112.txt

JSPWiki 2.5.[01;31m[K139[m[K - 'Comment.jsp' Multiple Cross-Site
Scripting Vulnerabilities |
jsp/webapps/30610.txt

JSPWiki 2.5.[01;31m[K139[m[K - 'Diff.jsp' Multiple Cross-Site Scripting
Vulnerabilities | jsp/webapps/30613.txt

JSPWiki 2.5.[01;31m[K139[m[K - 'edit.jsp?edittime' Cross-Site Scripting
| jsp/webapps/30609.txt

JSPWiki 2.5.[01;31m[K139[m[K - 'Login.jsp' Multiple Cross-Site
Scripting Vulnerabilities |
jsp/webapps/30612.txt

JSPWiki 2.5.[01;31m[K139[m[K - 'NewGroup.jsp' Multiple Cross-Site
Scripting Vulnerabilities |
jsp/webapps/30608.txt

JSPWiki 2.5.[01;31m[K139[m[K - 'UserPreferences.jsp' Multiple Cross-
Site Scripting Vulnerabilities |
jsp/webapps/30611.txt

K-Search - SQL Injection / Cross-Site Scripting
| php/webapps/[01;31m[K139[m[K93.txt

Kiasabz Article News CMS Magazine - SQL Injection
| php/webapps/12[01;31m[K139[m[K.txt

KubeLance 1.7.6 - 'profile.php' SQL Injection
| php/webapps/[01;31m[K139[m[K31.txt

Larson Network Print Server 9.4.2 build 105 - 'LstNPS' Logging Function
USEP Command Remote Format String | windows/dos/31[01;31m[K139[m[K.txt

Liferay Enterprise Portal 1.x/2.x/5.0.2 - Multiple Cross-Site Scripting
Vulnerabilities | jsp/webapps/24[01;31m[K139[m[K.txt

Lighttpd 1.4.x - mod_userdir Information Disclosure
| linux/remote/3[01;31m[K139[m[K6.txt

```
Linker IMG 1.0 - Remote File Inclusion
| php/webapps/[01;31m[K139[m[K64.txt

Linux Kernel 2.6.9 < 2.6.11 (RHEL 4) - 'SYS_EPoll_Wait' Local Integer
Overflow / Local Privilege Escalatio | linux/local/[01;31m[K139[m[K7.c

Live CMS - SQL Injection
| php/webapps/[01;31m[K139[m[K11.txt

Mambo Component Portfolio Manager 1.0 - 'categoryId' SQL Injection
| php/webapps/5[01;31m[K139[m[K.txt

MarketSaz - Arbitrary File Upload
| php/webapps/[01;31m[K139[m[K27.txt

Mars Stealer 8.3 - Admin Account Takeover
| php/webapps/5[01;31m[K139[m[K2.py

MAXdev My eGallery Module 3.04 - For Xoops 'gid' SQL Injection
| php/webapps/3[01;31m[K139[m[K2.txt

McAfee Framework ePolicy 3.x - Orchestrator '_naimcomn_Log' Remote
Format String                              |
windows/dos/3[01;31m[K139[m[K9.txt

Microsoft IIS - HTTP Request Denial of Service
| windows/dos/[01;31m[K139[m[K6.cpp

Microsoft Internet Explorer 6 - 'mshtml.dll div' Denial of Service
| windows/dos/[01;31m[K139[m[K4.html

Microsoft Windows XP/2003 - Metafile Escape() Code Execution
(Metasploit)                                       |
windows/remote/[01;31m[K139[m[K1.pm

Mini CMS 1.1 - Authentication Bypass
| php/webapps/41[01;31m[K139[m[K.txt

MoreAmp - '.maf' Buffer Overflow (PoC)
| windows/dos/[01;31m[K139[m[K34.py

MoreAmp - '.maf' Local Stack Buffer Overflow (SEH)
| windows/local/[01;31m[K139[m[K42.pl

Multi-Vendor Online Groceries Management System 1.0 - Remote Code
Execution                                  |
php/webapps/5[01;31m[K139[m[K4.py

My Little Homepage Products - BBCode Link Tag Script Injection
| php/webapps/27[01;31m[K139[m[K.txt

MyBB Transactions Plugin - 'transaction' SQL Injection
| php/webapps/38[01;31m[K139[m[K.txt
```

```
myPHP Guestbook 2.0.4 - Database Backup Dump
| php/webapps/1[01;31m[K139[m[K9.txt

myServer 0.4.x - 'cgi-lib.dll' Remote Buffer Overflow (PoC)
| windows/dos/23[01;31m[K139[m[K.txt

myUPB 2.2.6 - Multiple Vulnerabilities
| php/webapps/[01;31m[K139[m[K57.txt

Netgear DGN2200v1/v2/v3/v4 - 'ping.cgi' Remote Command Execution
| hardware/webapps/4[01;31m[K139[m[K4.py

Netware - SMB Remote Stack Overflow (PoC)
| novell/dos/[01;31m[K139[m[K06.txt

Omnidocs - SQL Injection
| jsp/webapps/1[01;31m[K139[m[K3.txt

Online Classified System Script - SQL Injection / Cross-Site Scripting
| php/webapps/[01;31m[K139[m[K67.txt

OpenSMTPD 6.6.3 - Arbitrary File Read
| linux/remote/48[01;31m[K139[m[K.c

Orbital Viewer 1.04 - '.ov' Local Universal Stack Overflow (SEH)
| windows/local/[01;31m[K139[m[K40.pl

OroHYIP - SQL Injection
| php/webapps/[01;31m[K139[m[K48.txt

Overstock Script - SQL Injection
| php/webapps/[01;31m[K139[m[K46.txt

Pandora FMS 7.0 NG 749 - Multiple Persistent Cross-Site Scripting
Vulnerabilities                          |
php/webapps/49[01;31m[K139[m[K.txt

PaperCut NG/MG 22.0.4 - Authentication Bypass
| multiple/webapps/5[01;31m[K139[m[K1.py

PenPals - Authentication Bypass
| php/webapps/[01;31m[K139[m[K01.txt

PHP Calendars Script - SQL Injection
| php/webapps/[01;31m[K139[m[K47.txt

PHP Captcha Security Images - Denial of Service
| php/dos/1[01;31m[K139[m[K7.txt

PHP Event Calendar 1.5 - Multiple Vulnerabilities
| php/webapps/[01;31m[K139[m[K88.txt
```

PHP Restaurants 1.0 - SQLi Authentication Bypass & Cross Site Scripting
| php/webapps/5[01;31m[K139[m[K8.txt

PHP-Nuke Module print 6.0 - 'print&sid' SQL Injection
| php/webapps/[01;31m[K139[m[K16.txt

PHPCodeCabinet 0.5 - 'Core.php' Remote File Inclusion
| php/webapps/2[01;31m[K139[m[K.txt

PHPDirector 0.21 - 'videos.php?id' SQL Injection
| php/webapps/4[01;31m[K139[m[K.txt

phpDocumentor 1.3.0 rc4 - Remote Command Execution
| php/webapps/[01;31m[K139[m[K5.php

PHPFox - Access Control Security Bypass
| php/webapps/39[01;31m[K139[m[K.txt

phpMyFAQ v3.1.12 - CSV Injection
| php/webapps/5[01;31m[K139[m[K9.txt

PHPShell 2.4 - Session Fixation
| php/webapps/4[01;31m[K139[m[K6.txt

PHPWCMS 1.4.5 r398 - Cross-Site Request Forgery
| php/webapps/[01;31m[K139[m[K60.html

Planet 1.1 - Cross-Site Request Forgery (Add Admin)
| php/webapps/[01;31m[K139[m[K04.txt

PowerZip 7.21 (Build 4010) - Stack Buffer Overflow
| windows/dos/[01;31m[K139[m[K21.c

Pre PHP Classifieds - SQL Injection
| php/webapps/[01;31m[K139[m[K92.txt

PreProject Multi-Vendor Shopping Malls - 'products.php?sid' SQL
Injection |
php/webapps/[01;31m[K139[m[K96.txt

PreProject Multi-Vendor Shopping Malls - SQL Injection
| php/webapps/[01;31m[K139[m[K87.txt

PVote 1.0/1.5 - Poll Content Manipulation
| php/webapps/2[01;31m[K139[m[K1.txt

PVote 1.0/1.5 - Unauthorized Administrative Password Change
| php/webapps/2[01;31m[K139[m[K7.txt

RadASM 2.2.1.6 - '.rap' Local Buffer Overflow (PoC)
| windows/dos/1[01;31m[K139[m[K2.c

```
ritsblog 0.4.2 - Authentication Bypass / Cross-Site Scripting
| php/webapps/8[01;31m[K139[m[K.txt

RSA Authentication Manager 8.2.1.4.0-build[01;31m[K139[m[K4922 / < 8.3
P1 - XML External Entity Injection / Cross-Site  |
java/webapps/44634.txt

RSS News AutoPilot Script 1.0.1/3.0.3 - Cross-Site Request Forgery
| php/webapps/4[01;31m[K139[m[K2.html

Saffa Tunes CMS - 'news.php' SQL Injection
| php/webapps/[01;31m[K139[m[K52.txt

Sambar Server 5.1 - Script Source Disclosure
| cgi/remote/2[01;31m[K139[m[K0.txt

Sawmill Enterprise 8.7.9 - Authentication Bypass
| windows/webapps/4[01;31m[K139[m[K5.txt

Shareasale Script - SQL Injection
| php/webapps/[01;31m[K139[m[K49.txt

Shopping Cart Script with Affiliate Program - SQL Injection
| php/webapps/[01;31m[K139[m[K30.txt

SimpleAssets - Authentication Bypass / Cross-Site Scripting
| php/webapps/[01;31m[K139[m[K44.txt

SnowCade 3.0 - SQL Injection
| php/webapps/[01;31m[K139[m[K37.txt

Social Community Script - SQL Injection
| php/webapps/[01;31m[K139[m[K77.txt

SoftBiz Banner Exchange Script 1.0 - 'gen_confirm_mem.php?PHPSESSID'
Cross-Site Scripting                  |
php/webapps/28[01;31m[K139[m[K.txt

Softbiz PHP FAQ Script - Blind SQL Injection
| php/webapps/[01;31m[K139[m[K91.txt

Softbiz Resource Repository Script - Blind SQL Injection
| php/webapps/[01;31m[K139[m[K86.txt

Software Index - Arbitrary File Upload
| php/webapps/[01;31m[K139[m[K99.html

SonicWALL email security 7.3.5 - Multiple Vulnerabilities
| windows/webapps/2[01;31m[K139[m[K4.txt

Sophos Web Appliance 4.3.10.4 - Pre-auth command injection
| php/webapps/5[01;31m[K139[m[K6.sh
```

SpiceWorks 6.0.00993 - Multiple Script Injection Vulnerabilities
| windows/webapps/2[01;31m[K139[m[K2.txt

Spring Framework - Arbitrary code Execution
| multiple/webapps/[01;31m[K139[m[K18.txt

SSH2 3.0 - Restricted Shell Escape (Command Execution)
| linux/local/2[01;31m[K139[m[K8.txt

Subtitle Translation Wizard 3.0.0 - Overflow (SEH) (PoC)
| windows/dos/[01;31m[K139[m[K65.py

Sun JDK 1.1.x / Sun JRE 1.1.x - Listening Socket
| multiple/remote/20[01;31m[K139[m[K.txt

Sysax Multi Server < 5.25 (SFTP Module) - Multiple Denial of Service Vulnerabilities |
windows/dos/[01;31m[K139[m[K58.txt

TeamSpeak 3.0.0-beta25 - Multiple Vulnerabilities
| windows/dos/[01;31m[K139[m[K59.txt

The Uploader 2.0.4 - Remote File Disclosure
| php/webapps/[01;31m[K139[m[K66.txt

Top Sites Script - SQL Injection
| php/webapps/[01;31m[K139[m[K76.txt

torrenttrader 2.08 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K139[m[K6.txt

Twilio WEB To Fax Machine System Application 1.0 - SQL Injection
| php/webapps/46[01;31m[K139[m[K.txt

UK One Media CMS - 'id' Error-Based SQL Injection
| php/webapps/[01;31m[K139[m[K33.txt

UNA CMS 14.0.0-RC - PHP Object Injection
| multiple/webapps/52[01;31m[K139[m[K.txt

vBulletin 2.3.x - SQL Injection
| php/webapps/1[01;31m[K139[m[K6.txt

vBulletin 3.0.0 - Cross-Site Scripting
| php/webapps/1[01;31m[K139[m[K5.txt

vBulletin 3.5.2 - Cross-Site Scripting
| php/webapps/1[01;31m[K139[m[K4.txt

Video Community portal - SQL Injection / Cross-Site Scripting
| php/webapps/[01;31m[K139[m[K70.txt

```
Vivotek IP Cameras - Multiple Vulnerabilities
| hardware/webapps/25[01;31m[K139[m[K.txt

Web Ofisi E-Ticaret 3 - 'a' SQL Injection
| linux/webapps/47[01;31m[K139[m[K.txt

Webring Script - SQL Injection
| php/webapps/[01;31m[K139[m[K75.txt

WebsiteBaker 2.8.1 - Cross-Site Request Forgery
| php/webapps/[01;31m[K139[m[K38.html

WebWiz Products 1.0/3.06 - Authentication Bypass / SQL Injection
| asp/webapps/[01;31m[K139[m[K9.txt

Winamp 5.05 < 5.13 - '.ini' Local Stack Buffer Overflow
| windows/local/11[01;31m[K139[m[K.c

Winamp 5.572 - Local Buffer Overflow (EIP + SEH) (DEP Bypass)
| windows/local/[01;31m[K139[m[K07.py

Wondershare Filmora 12.2.9.2233 - Unquoted Service Path
| windows/local/5[01;31m[K139[m[K5.txt

WordPress Plugin Mimetic Books 0.2.13 - 'Default Publisher ID field'
Stored Cross-Site Scripting (XSS)     |
php/webapps/50[01;31m[K139[m[K.txt

WordPress Plugin wp-topbar 4.02 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K139[m[K3.txt

---------------------------------------------------------------------------------------------- ----------------
----------

---------------------------------------------------------------------------------------------- ----------------
----------
Shellcode Title
|  Path

---------------------------------------------------------------------------------------------- ----------------
----------
Linux/ARM - Disable ASLR Security Shellcode (102 bytes)
| arm/14[01;31m[K139[m[K.c

Linux/x64 - Add Root User (shell-storm/leet) To /etc/{passwd_shadow}
Shellcode (390 bytes)                 | linux_x86-
64/[01;31m[K139[m[K43.c

Linux/x64 - Disable ASLR Security Shellcode (143 bytes)
| linux_x86-64/[01;31m[K139[m[K08.c
```

Linux/x64 - Reverse (10.1.1.4:46357/TCP) Shell + Subtle Probing + Timer + Burst + Password (la crips) + Mu | linux_x86-64/40[01;31m[K139[m[K.c

Linux/x64 - Reverse (127.0.0.1:4444/TCP) Shell (/bin/sh) Shellcode (65 bytes) | linux_x86-64/4[01;31m[K139[m[K8.nasm

Linux/x64 - Reverse (127.1.1.1:6969/TCP) Shell (/bin/bash) Shellcode ([01;31m[K139[m[K bytes) | linux_x86-64/34667.c

Linux/x64 - setuid(0) + chmod (/etc/passwd 0777) + exit(0) Shellcode (63 bytes) | linux_x86-64/[01;31m[K139[m[K15.c

Linux/x86 - Bind (31337/TCP) Shell + setreuid(0_0) + Polymorphic Shellcode (131 bytes) | linux_x86/[01;31m[K139[m[K10.c

Linux/x86 - Reverse (::FFFF:192.168.1.5:4444/TCP) Shell (/bin/sh) + Null-Free + IPv6 Shellcode (86 bytes) | linux_x86/45[01;31m[K139[m[K.c

Windows/x64 - Delete File shellcode / Dynamic PEB method null-free Shellcode | windows/5[01;31m[K139[m[K0.asm

---

Port: 2049

Exploit Title
| Path

Apple macOS/iOS - Memory Corruption Due to Bad Bounds Checking in NSCharacterSet Coding for NSKeyedUnarchi | multiple/dos/4[01;31m[K2049[m[K.txt

BitchX IRC Client 1.0 c17 - DNS Buffer Overflow
| unix/remote/[01;31m[K2049[m[K0.c

KTH Kerberos 4 - Arbitrary Proxy Usage
| multiple/remote/[01;31m[K2049[m[K1.txt

Leif M. Wright everythingform.cgi 2.0 - Arbitrary Command Execution
| cgi/remote/[01;31m[K2049[m[K7.html

Lib CGI 0.1 - Include Buffer Overflow
| unix/remote/2[01;31m[K2049[m[K.c

Microsoft Internet Explorer 6 - New ActiveX Object String Concatenation Memory Corruption |
windows/remote/3[01;31m[K2049[m[K.txt

Oops Proxy Server 1.4.22 - Remote Buffer Overflow (1)
| unix/remote/[01;31m[K2049[m[K5.c

Oops Proxy Server 1.4.22 - Remote Buffer Overflow (2)
| linux/remote/[01;31m[K2049[m[K6.c

RedHat Linux 7.0 - Roaring Penguin PPPoE Denial of Service
| linux/dos/[01;31m[K2049[m[K4.pl

SiteDepth CMS 3.0.1 - 'SD_DIR' Remote File Inclusion
| php/webapps/[01;31m[K2049[m[K.txt

ssldump 0.9 b1 - Format String
| unix/remote/[01;31m[K2049[m[K2.txt

Uiga Proxy - Remote File Inclusion
| php/webapps/1[01;31m[K2049[m[K.html

University of Washington Pico 3.x/4.x - File Overwrite
| linux/local/[01;31m[K2049[m[K3.sh

Shellcodes: No Results

Port: 21

Exploit Title
| Path

(Tod Miller's) Sudo/SudoEdit 1.6.9p[01;31m[K21[m[K/1.7.2p4 - Local Privilege Escalation |
multiple/local/11651.sh

.netCART Settings.XML - Information Disclosure
| asp/webapps/229[01;31m[K21[m[K.txt

1 Click Audio Converter 2.3.6 - Activex Local Buffer Overflow
| windows/local/37[01;31m[K21[m[K1.html

```
1 Click Extract Audio 2.3.6 - Activex Buffer Overflow
| windows/local/37[01;31m[K21[m[K2.html

1-Script 1-Search 1.8 - '1search.CGI' Cross-Site Scripting
| cgi/webapps/267[01;31m[K21[m[K.txt

123 Flash Chat 5.0 - Remote Code Injection
| php/webapps/271[01;31m[K21[m[K.txt

[01;31m[K21[m[K2Cafe Board 0.07 - 'qID' SQL Injection
| php/webapps/6578.txt

[01;31m[K21[m[K2Cafe Board 0.08 Beta / 6.30 Beta - Multiple Cross-Site
Scripting Vulnerabilities                          |
php/webapps/29505.txt

[01;31m[K21[m[K2Cafe Guestbook 4.00 - 'show.php' Cross-Site Scripting
| php/webapps/29507.txt

[01;31m[K21[m[K2Cafe WebBoard 2.90 Beta - 'view.php' Directory
Traversal                                                  |
php/webapps/34940.txt

[01;31m[K21[m[K2Cafe WebBoard 2.90 Beta - Remote File Disclosure
| php/webapps/8823.txt

[01;31m[K21[m[K2Cafe WebBoard 6.30 - 'Read.php' SQL Injection
| php/webapps/30560.txt

3.3/4.0/4.2 MERCUR MailServer - Control-Service Buffer Overflow
| windows/remote/[01;31m[K21[m[K626.c

3[01;31m[K21[m[Ksoft PHP-Gallery 0.9 - 'index.php?path' Arbitrary
Directory Listing                                      |
php/webapps/27803.txt

3[01;31m[K21[m[Ksoft PHP-Gallery 0.9 - 'index.php?path' Cross-Site
Scripting                                              |
php/webapps/27804.txt

32bit FTP (09.04.24) - 'CWD Response' Universal Overwrite (SEH)
| windows_x86/remote/86[01;31m[K21[m[K.py

3CDaemon 2.0 - Buffer Overflow (1)
| windows/dos/[01;31m[K21[m[K429.c

3Com SuperStack II PS Hub 40 - TelnetD Weak Password Protection
| hardware/remote/[01;31m[K21[m[K011.pl

3D-FTP 8.01 - 'LIST' / 'MLSD' Directory Traversal
| multiple/remote/319[01;31m[K21[m[K.txt
```

```
3proxy 0.5.3g (Linux) - 'proxy.c logurl()' Remote Buffer Overflow
| linux/remote/38[01;31m[K21[m[K.c

4Images 1.7.9 - Multiple Remote File Inclusions / SQL Injections
| php/webapps/356[01;31m[K21[m[K.txt

602Pro LAN SUITE 2002 - Telnet Proxy localhost Denial of Service
| windows/dos/[01;31m[K21[m[K694.pl

68kb 68KB Base 1.0.0rc3 - Cross-Site Request Forgery (Admin)
| php/webapps/120[01;31m[K21[m[K.txt

6Tunnel 0.6/0.7/0.8 - Connection Close State Denial of Service
| multiple/dos/[01;31m[K21[m[K126.c

8E6 Technologies R3000 - Host Header Internet Filter Security Bypass
| multiple/remote/3[01;31m[K21[m[K67.txt

aaPanel 6.8.[01;31m[K21[m[K - Directory Traversal (Authenticated)
| linux/webapps/50780.txt

Abac Karaoke 2.15 - Denial of Service
| windows/dos/146[01;31m[K21[m[K.py

ABB Cylon Aspect 3.07.01 - Hard-coded Default Credentials
| php/webapps/5[01;31m[K21[m[K12.NA

ABB Cylon Aspect 3.07.02 (userManagement.php) - Weak Password Policy
| multiple/hardware/522[01;31m[K21[m[K.txt

ABB Cylon Aspect 3.07.02 - File Disclosure
| multiple/webapps/5[01;31m[K21[m[K15.NA

ABB Cylon Aspect 3.08.01 - Arbitrary File Delete
| php/webapps/5[01;31m[K21[m[K08.NA

ABB Cylon Aspect 3.08.01 - Remote Code Execution (RCE)
| multiple/webapps/5[01;31m[K21[m[K07.NA

ABB Cylon Aspect 3.08.02 (bbmdUpdate.php) - Remote Code Execution
| multiple/hardware/52[01;31m[K21[m[K7.txt

ABB Cylon Aspect 3.08.02 (escDevicesUpdate.php) - Denial of Service
(DOS)                                   |
php/hardware/52[01;31m[K21[m[K8.txt

ABB Cylon Aspect 3.08.02 (licenseServerUpdate.php) - Stored Cross-Site
Scripting                               |
multiple/hardware/52[01;31m[K21[m[K4.txt

ABB Cylon Aspect 3.08.02 (licenseUpload.php) - Stored Cross-Site
Scripting                                       |
multiple/hardware/52[01;31m[K21[m[K5.txt
```

ABB Cylon Aspect 3.08.02 (uploadDb.php) - Remote Code Execution
| multiple/hardware/52[01;31m[K21[m[K6.txt

ABB Cylon Aspect 3.08.02 (webServerUpdate.php) - Input Validation
Config Poisoning |
php/hardware/52[01;31m[K21[m[K9.txt

ABB Cylon Aspect 3.08.02 - PHP Session Fixation
| multiple/hardware/5[01;31m[K21[m[K82.txt

ABB Cylon FLXeon 9.3.4 - Cross-Site Request Forgery
| multiple/hardware/5[01;31m[K21[m[K80.txt

ABB Cylon FLXeon 9.3.4 - Default Credentials
| multiple/hardware/5[01;31m[K21[m[K79.txt

ABB Cylon FLXeon 9.3.4 - Remote Code Execution (Authenticated)
| multiple/hardware/5[01;31m[K21[m[K88.txt

ABB Cylon FLXeon 9.3.4 - Remote Code Execution (RCE)
| multiple/hardware/5[01;31m[K21[m[K86.txt

ABB Cylon FLXeon 9.3.4 - System Logs Information Disclosure
| multiple/hardware/5[01;31m[K21[m[K78.txt

ABB Cylon FLXeon 9.3.4 - WebSocket Command Spawning
| multiple/hardware/5[01;31m[K21[m[K84.txt

ABCPP 1.3 - Directive Handler Buffer Overflow
| windows/remote/250[01;31m[K21[m[K.txt

Abe Timmerman - 'zml.cgi' File Disclosure
| cgi/remote/[01;31m[K21[m[K194.txt

Ability Mail Server 2013 -Persistent Cross-Site Scripting / Cross-Site
Request Forgery (Password Reset) |
windows/webapps/312[01;31m[K21[m[K.txt

AbleDesign MyCalendar 2.20.3 - 'index.php' Multiple Cross-Site
Scripting Vulnerabilities |
php/webapps/296[01;31m[K21[m[K.txt

Abrt (Fedora [01;31m[K21[m[K) - Race Condition
| linux/local/36747.c

ABRT - sosreport Privilege Escalation (Metasploit)
| linux/local/474[01;31m[K21[m[K.rb

AbsoluteTelnet 11.[01;31m[K21[m[K - 'Username' Denial of Service (PoC)
| windows/dos/48493.py

ABUS Security Camera TVIP 20000-[01;31m[K21[m[K150 - LFI_ RCE and SSH Root Access |
hardware/remote/51294.txt

Abuse 2.0 - Local Buffer Overflow
| linux/local/[01;31m[K21[m[K980.c

Abyss Web Server 1.0 - Encoded Backslash Directory Traversal
| windows/remote/[01;31m[K21[m[K735.txt

Abyss Web Server 1.0 - File Disclosure
| windows/remote/[01;31m[K21[m[K367.txt

Accela Civic Platform [01;31m[K21[m[K.1 - 'contactSeqNumber' Insecure Direct Object References (IDOR) |
multiple/webapps/49991.txt

Accela Civic Platform [01;31m[K21[m[K.1 - 'servProvCode' Cross-Site-Scripting (XSS) |
multiple/webapps/49980.txt

Accela Civic Platform [01;31m[K21[m[K.1 - 'successURL' Cross-Site-Scripting (XSS) |
multiple/webapps/49990.txt

Achievo 0.7/0.8/0.9 - Remote File Inclusion / Command Execution
| php/webapps/[01;31m[K21[m[K745.txt

ACME Labs thttpd 2.20 - Cross-Site Scripting
| linux/remote/[01;31m[K21[m[K422.txt

Acoustica MP3 Audio Mixer 2.471 - '.m3u' Local Heap Overflow (PoC)
| windows/dos/9[01;31m[K21[m[K3.pl

Acoustica MP3 Audio Mixer 2.471 - '.sgp' Crash
| windows/dos/9[01;31m[K21[m[K2.pl

ActFax Server (LPD/LPR) 4.25 Build 02[01;31m[K21[m[K (2010-02-11) - Remote Buffer Overflow |
windows/remote/16176.pl

ActFax Server FTP 4.25 Build 02[01;31m[K21[m[K (2010-02-11) - (Authenticated) Remote Buffer Overflow |
windows/remote/16177.py

Active CMS 1.2 - 'mod' Cross-Site Scripting
| php/webapps/36[01;31m[K21[m[K3.txt

Active eCommerce CMS 6.5.0 - Stored Cross-Site Scripting (XSS)
| multiple/webapps/512[01;31m[K21[m[K.txt

ActiveFax (ActFax) 4.3 - Client Importer Buffer Overflow (Metasploit)
| windows/local/[01;31m[K21[m[K139.rb

```
ActivePerl 5.6.1 - 'perlIIS.dll' Remote Buffer Overflow (1)
| linux/remote/[01;31m[K21[m[K152.c

ActivePerl 5.6.1 - 'perlIIS.dll' Remote Buffer Overflow (2)
| windows/remote/[01;31m[K21[m[K153.c

ActivePerl 5.6.1 - 'perlIIS.dll' Remote Buffer Overflow (3)
| multiple/remote/[01;31m[K21[m[K154.pl

ACWeb 1.14/1.8 - Cross-Site Scripting
| linux/remote/[01;31m[K21[m[K858.txt

Adaware Web Companion 4.9.[01;31m[K21[m[K59 - 'WCAssistantService'
Unquoted Service Path                                  |
windows/local/47852.txt

Adianti Framework 5.5.0 - SQL Injection
| php/webapps/46[01;31m[K21[m[K7.txt

Adive Framework 2.0.7 - Cross-Site Request Forgery
| php/webapps/47[01;31m[K21[m[K7.txt

ADM 3.1.2RHG1 - Remote Code Execution
| hardware/webapps/45[01;31m[K21[m[K2.py

AdMan 1.0.200512[01;31m[K21[m[K - 'ViewStatement.php' SQL Injection
| php/webapps/27462.txt

ADManager 1.1 - Content Manipulation
| php/webapps/[01;31m[K21[m[K424.txt

Admidio 2.3.5 - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K005.txt

Admiral Systems EmailClub 1.0.0.5 - Remote Buffer Overflow
| windows/remote/196[01;31m[K21[m[K.c

Adobe Acrobat and Reader - Array Indexing Remote Code Execution
| osx/dos/15[01;31m[K21[m[K2.txt

Adobe ColdFusion 9 - Administrative Authentication Bypass (Metasploit)
| multiple/remote/30[01;31m[K21[m[K0.rb

Adobe ColdFusion versions 2018_15 (and earlier) and 20[01;31m[K21[m[K_5
and earlier - Arbitrary File Read                      |
multiple/webapps/51875.py

Adobe eBook Reader 2.2 - File Restoration Privilege Escalation
| windows/local/[01;31m[K21[m[K629.txt

Adobe Flash - Crash When Freeing Memory After AVC decoding
| multiple/dos/404[01;31m[K21[m[K.txt
```

```
Adobe Flash - SWF Stack Corruption
| multiple/dos/414[01;31m[K21[m[K.txt

Adobe Flash - Use-After-Free When Setting Stage
| windows_x86-64/dos/392[01;31m[K21[m[K.txt

Adobe Flash BlurFilter Processing - Out-of-Bounds Memset
| multiple/dos/39[01;31m[K21[m[K9.txt

Adobe Flash MovieClip.lineStyle - Use-After-Frees
| windows/dos/390[01;31m[K21[m[K.txt

Adobe Flash Player - Integer Underflow Remote Code Execution
(Metasploit)                                  |
windows/remote/33[01;31m[K21[m[K2.rb

Adobe Reader 10.1.4 - Crash (PoC)
| windows/dos/2[01;31m[K21[m[K55.pl

Adobe Reader 9.3.2 - 'CoolType.dll' Remote Memory Corruption / Denial
of Service                            |
multiple/dos/141[01;31m[K21[m[K.c

Advanced Matrimonial Script 2.0.3 - SQL Injection
| php/webapps/415[01;31m[K21[m[K.txt

Advertiz PHP Script 0.2 - Cross-Site Request Forgery (Update Admin)
| php/webapps/426[01;31m[K21[m[K.html

Aerohive HiveOS 5.1r5 < 6.1r5 - Remote Code Execution
| hardware/webapps/4[01;31m[K21[m[K78.py

Aestiva HTML/OS 2.4 - Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K769.txt

AFCommerce - 'adminpassword.php' Remote File Inclusion
| php/webapps/389[01;31m[K21[m[K.txt

AFD 1.2.x - Working Directory Local Buffer Overflow / Local Privilege
Escalation                            | unix/local/[01;31m[K21[m[K771.c

Agares phpAutoVideo 2.[01;31m[K21[m[K - 'articlecat' SQL Injection (1)
| php/webapps/4898.txt

Agares phpAutoVideo 2.[01;31m[K21[m[K - 'articlecat' SQL Injection (2)
| php/webapps/4905.pl

Agares phpAutoVideo 2.[01;31m[K21[m[K - Local/Remote File Inclusion
| php/webapps/4782.txt

Agora.CGI 3.x/4.0 - Debug Mode Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K184.txt
```

Agora.CGI 3/4 - Debug Mode Full Path Disclosure
| cgi/remote/[01;31m[K21[m[K249.txt

AHG Search Engine 1.0 - 'search.cgi' Arbitrary Command Execution
| cgi/webapps/[01;31m[K21[m[K257.txt

Aimeos Laravel ecommerce platform 20[01;31m[K21[m[K.10 LTS - 'sort' SQL injection | php/webapps/50538.txt

AIOCP 1.3.x - 'cp_links_search.php' Cross-Site Scripting
| php/webapps/289[01;31m[K21[m[K.txt

Aircrack-NG Tools svn r1675 - Remote Heap Buffer Overflow (PoC)
| multiple/dos/12[01;31m[K21[m[K7.py

AirDisk Pro 5.5.3 for iOS - Persistent Cross-Site Scripting
| ios/webapps/483[01;31m[K21[m[K.txt

airVisionNVR 1.1.13 - 'readfile()' Disclosure / SQL Injection
| php/webapps/[01;31m[K21[m[K990.txt

AIX 4.1/4.2 - 'pdnsd' Remote Buffer Overflow
| aix/remote/[01;31m[K21[m[K093.c

AIX 4.2/4.3 - '/usr/lib/lpd/pio/etc/piomkapqd' Local Buffer Overflow
| aix/local/[01;31m[K21[m[K094.c

AIX 4.2/4.3 - netstat -Z Statistic Clearing
| aix/local/20[01;31m[K21[m[K3.txt

AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode [01;31m[K21[m[K - Buffer Overflow (Metasploit) | aix/dos/16929.rb

Ajax File Manager - Directory Traversal
| php/webapps/3[01;31m[K21[m[K15.txt

Ajax PHP Penny Auction 1.x 2.x - Multiple Vulnerabilities
| php/webapps/275[01;31m[K21[m[K.txt

AjaXplorer - 'checkInstall.php' Remote Command Execution (Metasploit)
| php/remote/[01;31m[K21[m[K993.rb

akcms 4.2.4 - Information Disclosure
| php/webapps/[01;31m[K21[m[K251.txt

Aktivate 1.0 3 - Shopping Cart Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K187.txt

Aladdin eToken PKI Client 4.5 - Virtual File Handling Memory Corruption (PoC) | windows/dos/1[01;31m[K21[m[K61.pl

```
Alcatel OmniPCX Office [01;31m[K21[m[K0/061.1 - Remote Command
Execution                                                    |
cgi/webapps/5662.txt

Alibaba-clone CMS - SQL Injection / Blind SQL Injection
| php/webapps/9[01;31m[K21[m[K1.txt

Alleged Outlook Express 5/6 Link - Denial of Service
| windows/dos/[01;31m[K21[m[K789.txt

Alleycode 2.[01;31m[K21[m[K - Local Overflow (SEH)
| windows/local/9991.txt

Allok AVI DivX MPEG to DVD Converter 2.6.1[01;31m[K21[m[K7 - Buffer
Overflow (SEH)                                              |
windows/local/44363.py

Allok AVI to DVD SVCD VCD Converter 4.0.1[01;31m[K21[m[K7 - Buffer
Overflow (SEH)                                              |
windows/local/44549.py

Allok MOV Converter 4.6.1[01;31m[K21[m[K7 - Buffer Overflow (SEH)
| windows/local/45101.py

Allok QuickTime to AVI MPEG DVD Converter 3.6.1[01;31m[K21[m[K7 -
Buffer Overflow                                             |
windows/dos/44273.py

Allok Quicktime to AVI MPEG DVD Converter 4.6.1[01;31m[K21[m[K7 -
Stack-Based Buffer Overflow                                 |
windows/local/44330.py

Allok RM RMVB to AVI MPEG DVD Converter 3.6.1[01;31m[K21[m[K7 - Stack
Overflow (SEH)                                              |
windows/local/47910.py

Allok Video Converter 4.6.1[01;31m[K21[m[K7 - Stack Overflow (SEH)
| windows/local/47908.py

Allok Video Joiner 4.6.1[01;31m[K21[m[K7 - Stack-Based Buffer Overflow
| windows/local/44364.py

Allok Video to DVD Burner 2.6.1[01;31m[K21[m[K7 - Buffer Overflow (SEH)
| windows/local/44518.py

Allok WMV to AVI MPEG DVD WMV Converter 4.6.1[01;31m[K21[m[K7 - Buffer
Overflow                                                    |
windows/local/44365.py

AlphAdmin CMS 1.0.5_03 - 'aa_login' Cookie Authentication Bypass
| php/webapps/3[01;31m[K21[m[K02.txt
```

```
AlsaPlayer 0.99.71 - Local Buffer Overflow
| linux/local/[01;31m[K21[m[K814.c

Alstrasoft AskMe Pro 2.1 - Multiple SQL Injections
| php/webapps/58[01;31m[K21[m[K.txt

Alstrasoft e-Friends 4.[01;31m[K21[m[K - Admin Session Retrieve
| php/webapps/3956.php

Alstrasoft Live Support 1.[01;31m[K21[m[K - Admin Credential Retrieve
| php/webapps/3957.php

Alt-N MDaemon 6.0.x - POP Server Buffer Overflow
| windows/dos/[01;31m[K21[m[K965.txt

Alt-N WebAdmin 2.0.4 - USER Buffer Overflow (Metasploit)
| windows/remote/1[01;31m[K21[m[K0.pm

Alteon AceDirector - Half-Closed HTTP Request IP Address Revealing
| hardware/remote/[01;31m[K21[m[K243.pl

Amanda 3.3.1 - Local Privilege Escalation
| linux/local/39[01;31m[K21[m[K7.c

Amaya 11.1 - W3C Editor/Browser 'defer' Remote Stack Overflow
| windows/remote/83[01;31m[K21[m[K.py

AmazCart CMS 3.4 - Cross-Site-Scripting (XSS)
| php/webapps/51[01;31m[K21[m[K9.txt

Ampache 3.4.3 - 'login.php' Multiple SQL Injections
| php/webapps/334[01;31m[K21[m[K.txt

Amtote Homebet - Account Information Brute Force
| multiple/remote/[01;31m[K21[m[K116.pl

AmTote Homebet - World Accessible Log
| multiple/remote/[01;31m[K21[m[K115.pl

AN HTTPD 1.38/1.39/1.40/1.41 - 'SOCKS4' Buffer Overflow
| windows/remote/[01;31m[K21[m[K955.java

AN HTTPD 1.41 e - Cross-Site Scripting
| multiple/remote/2[01;31m[K21[m[K30.txt

AnalogX Proxy 4.0 - Socks4A Buffer Overflow
| windows/remote/[01;31m[K21[m[K589.pl

AnalogX SimpleServer:WWW 1.16 - Web Server Buffer Overflow
| windows/remote/[01;31m[K21[m[K542.c
```

```
Android - ashmem Readonly Bypasses via remap_file_pages() and
ASHMEM_UNPIN                                    |
android/dos/479[01;31m[K21[m[K.txt

Andy Mack 35mm Slide Gallery 6.0 - 'popup.php' Multiple Cross-Site
Scripting Vulnerabilities               |
php/webapps/280[01;31m[K21[m[K.txt

Angular-Base64-Upload Library 0.1.20 - Remote Code Execution (RCE)
| multiple/remote/5[01;31m[K21[m[K[01;31m[K21[m[K.py

Angular-Base64-Upload Library 0.1.[01;31m[K21[m[K - Unauthenticated
Remote Code Execution (RCE)                             |
multiple/webapps/52253.py

Annuaire 1Two 1.0/1.1 - 'index.php' Cross-Site Scripting
| php/webapps/258[01;31m[K21[m[K.txt

Anti-Web HTTPd 2.2 Script - Engine File Opening Denial of Service
| linux/dos/[01;31m[K21[m[K202.txt

AnyBurn 4.8 - Buffer Overflow (SEH)
| windows/local/48[01;31m[K21[m[K1.py

Anyzip 1.1 - '.zip' (PoC) (SEH)
| windows/dos/1[01;31m[K21[m[K04.py

AOL Instant Messenger 4.8.2790 - Local File Execution
| windows/remote/[01;31m[K21[m[K958.txt

AOL Instant Messenger 4.x - Arbitrary File Creation
| windows/remote/[01;31m[K21[m[K386.html

AOL Instant Messenger 4.x - Hyperlink Denial of Service
| windows/dos/[01;31m[K21[m[K333.txt

AOL Instant Messenger 4.x - Remote Buffer Overflow
| windows/remote/[01;31m[K21[m[K196.txt

AOL Instant Messenger 4.x - Unauthorized Actions
| windows/remote/[01;31m[K21[m[K619.txt

AOLServer 3 - 'Authentication String' Remote Buffer Overflow (1)
| unix/remote/[01;31m[K21[m[K088.pl

AOLServer 3 - 'Authentication String' Remote Buffer Overflow (2)
| unix/remote/[01;31m[K21[m[K089.c

Apache - Denial of Service
| linux/dos/182[01;31m[K21[m[K.c

Apache 1.0/1.2/1.3 - Server Address Disclosure
| multiple/remote/[01;31m[K21[m[K067.c
```

Apache 1.3 - Directory Index Disclosure
| multiple/remote/[01;31m[K21[m[K002.txt

Apache 1.3.12 - WebDAV Directory Listings
| linux/remote/20[01;31m[K21[m[K0.txt

Apache 1.3.20 (Win32) - 'PHP.exe' Remote File Disclosure
| windows/remote/[01;31m[K21[m[K204.txt

Apache 1.3/2.0.x - Server Side Include Cross-Site Scripting
| multiple/remote/[01;31m[K21[m[K885.txt

Apache 1.x/2.0.x - Chunked-Encoding Memory Corruption (1)
| multiple/remote/[01;31m[K21[m[K559.c

Apache 1.x/2.0.x - Chunked-Encoding Memory Corruption (2)
| multiple/remote/[01;31m[K21[m[K560.c

Apache 2.0 - Encoded Backslash Directory Traversal
| windows/remote/[01;31m[K21[m[K697.txt

Apache 2.0 - Full Path Disclosure
| windows/remote/[01;31m[K21[m[K719.txt

Apache 2.0.39/40 - Oversized STDERR Buffer Denial of Service
| linux/dos/[01;31m[K21[m[K854.c

Apache < 2.0.64 / < 2.2.[01;31m[K21[m[K mod_setenvif - Integer Overflow
| linux/dos/41769.txt

Apache Axis2 1.4.1 - Local File Inclusion
| php/webapps/127[01;31m[K21[m[K.txt

Apache Geronimo 2.1.x - '/console/portal/' URI Cross-Site Scripting
| multiple/remote/329[01;31m[K21[m[K.txt

Apache HugeGraph Server 1.2.0 - Remote Code Execution (RCE)
| java/webapps/5[01;31m[K21[m[K49.py

Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow
| multiple/dos/[01;31m[K21[m[K575.txt

Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow
| unix/remote/[01;31m[K21[m[K671.c

Apache Subversion 1.6.x - 'mod_dav_svn/lock.c' Remote Denial of Service
| linux/dos/384[01;31m[K21[m[K.txt

Apache Tomcat 11.0.3 - Remote Code Execution
| multiple/webapps/5[01;31m[K21[m[K34.txt

Apache Tomcat 3.2 - Directory Disclosure
| unix/remote/[01;31m[K21[m[K882.txt

```
Apache Tomcat 3.2.3/3.2.4 - 'RealPath.jsp' Information Disclosuree
| multiple/remote/[01;31m[K21[m[K492.txt

Apache Tomcat 3.2.3/3.2.4 - 'Source.jsp' Information Disclosure
| multiple/remote/[01;31m[K21[m[K490.txt

Apache Tomcat 3.2.3/3.2.4 - Example Files Web Root Full Path Disclosure
| multiple/remote/[01;31m[K21[m[K491.txt

Apache Tomcat 3/4 - 'DefaultServlet' File Disclosure
| unix/remote/[01;31m[K21[m[K853.txt

Apache Tomcat 3/4 - JSP Engine Denial of Service
| linux/dos/[01;31m[K21[m[K534.jsp

Apache Tomcat 4.0.3 - Denial of Service 'Device Name' / Cross-Site
Scripting                                |
windows/webapps/[01;31m[K21[m[K605.txt

Apache Tomcat 4.0.3 - Servlet Mapping Cross-Site Scripting
| linux/remote/[01;31m[K21[m[K604.txt

Apache Tomcat 4.0/4.1 - Servlet Full Path Disclosure
| unix/remote/[01;31m[K21[m[K412.txt

Apache Tomcat 4.1 - JSP Request Cross-Site Scripting
| unix/remote/[01;31m[K21[m[K734.txt

Apache Tomcat 6.0.16 - 'HttpServletResponse.sendError()' Cross-Site
Scripting                                |
multiple/remote/3[01;31m[K21[m[K38.txt

Apache Tomcat 6.0.16 - 'RequestDispatcher' Information Disclosure
| multiple/remote/3[01;31m[K21[m[K37.txt

Apache Web Server 2.0.x - MS-DOS Device Name Denial of Service
| linux/dos/2[01;31m[K21[m[K91.pl

Apache Win32 1.3.x/2.0.x - Batch File Remote Command Execution
| windows/remote/[01;31m[K21[m[K350.pl

APC PowerChute Network Shutdown - HTTP Response Splitting / Cross-Site
Scripting                            |
java/webapps/328[01;31m[K21[m[K.html

Apple iOS 11.2.5 / watchOS 4.2.2 / tvOS 11.2.5 - 'bluetoothd' Memory
Corruption                             |
multiple/dos/44[01;31m[K21[m[K5.m

Apple iOS Mobile Mail - LibTIFF Buffer Overflow (Metasploit)
| ios/remote/[01;31m[K21[m[K869.rb
```

```
Apple iOS Mobile Safari - LibTIFF Buffer Overflow (Metasploit)
| ios/remote/[01;31m[K21[m[K868.rb

Apple Mac OS Internet Explorer 3/4/5 - File Execution
| osx/remote/[01;31m[K21[m[K238.txt

Apple Mac OSX 10.1.x - SoftwareUpdate Arbitrary Package Installation
| osx/remote/[01;31m[K21[m[K596.txt

Apple Mac OSX 10.2 - Terminal.APP Telnet Link Command Execution
| osx/local/[01;31m[K21[m[K815.txt

Apple Mac OSX 10.3.8 - 'CF_CHARSET_PATH' Local Buffer Overflow (2)
| osx/local/[01;31m[K21[m[K11.pl

Apple Mac OSX 10.3.x - Help Protocol Remote Code Execution
| osx/remote/241[01;31m[K21[m[K.txt

Apple Mac OSX 10.4.7 (PPC) - 'fetchmail' Local Privilege Escalation
| osx/local/[01;31m[K21[m[K07.pl

Apple Mac OSX 10.4.7 (x86) - 'fetchmail' Local Privilege Escalation
| osx/local/[01;31m[K21[m[K06.pl

Apple Mac OSX 10.4.7 - fetchmail Privilege Escalation
| osx/local/[01;31m[K21[m[K08.sh

Apple Mac OSX 10.4.8 (8L[01;31m[K21[m[K27) - 'crashdump' Local
Privilege Escalation                                    |
osx/local/3[01;31m[K21[m[K9.rb

Apple Mac OSX 10.x - CoreGraphics Multiple Memory Corruption
Vulnerabilities                                 |
osx/dos/3[01;31m[K21[m[K36.html

Apple Mac OSX 10.x / FreeBSD 4.x / OpenBSD 2.x / Solaris 2.5/2.6/7.0/8
- 'exec C Library' Standard I/O Fil | bsd/local/[01;31m[K21[m[K407.c

Apple macOS - Disk Arbitration Daemon Race Condition
| macos/local/4[01;31m[K21[m[K46.sh

Apple macOS 10.12.3 / iOS < 10.3.2 - Userspace Entitlement Checking
Race Condition                          |
multiple/local/4[01;31m[K21[m[K45.c

Apple macOS XNU Kernel - Memory Disclosure due to bug in Kernel API for
Detecting Kernel Memory Disclosure | macos/dos/433[01;31m[K21[m[K.c

Apple Open Firmware 4.1.7/4.1.8 - Insecure Password
| osx/local/[01;31m[K21[m[K070.txt

Apple QuickTime 5.0 - Content-Type Remote Buffer Overflow
| windows/remote/[01;31m[K21[m[K286.c
```

Apple QuickTime 6/7 - '.FLC' Movie COLOR_64 Chunk Overflow
| osx/dos/285[01;31m[K21[m[K.txt

Apple QuickTime Player 7.7.2 - Crash (PoC)
| windows/dos/22[01;31m[K21[m[K4.pl

Apple Safari 10.1 - Spread Operator Integer Overflow Remote Code Execution |
macos/remote/4[01;31m[K21[m[K25.txt

Apple Safari 2.0.4 - KHTML WebKit Remote Denial of Service
| osx/dos/310[01;31m[K21[m[K.html

Apple Safari 4.0.4 (531.[01;31m[K21[m[K.10) - Stack Overflow / Denial of Service |
windows/dos/11601.pl

Apple WebKit - 'HTMLFormElement::reset()' Use-After Free
| osx/dos/41[01;31m[K21[m[K3.html

Apple WebKit - 'HTMLKeygenElement' Type Confusion
| multiple/dos/41[01;31m[K21[m[K5.html

Apple WebKit - Type Confusion in RenderBox with Accessibility Enabled
| multiple/dos/41[01;31m[K21[m[K6.html

Apple WebKit 10.0.2 (12602.3.12.0.1_ r[01;31m[K21[m[K0800) - 'constructJSReadableStreamDefaultReader' Type Confusion |
multiple/webapps/41803.html

AppSmith 1.47 - Remote Code Execution (RCE)
| java/webapps/5[01;31m[K21[m[K18.py

Aptana Jaxer 1.0.3.4547 - Local File inclusion
| multiple/webapps/47[01;31m[K21[m[K4.txt

AquilaCMS 1.409.20 - Remote Command Execution (RCE)
| php/webapps/5[01;31m[K21[m[K64.py

Arctic Torrent 1.2.3 - Memory Corruption (Denial of Service)
| windows/dos/[01;31m[K21[m[K824.pl

ArGoSoft 1.8 Mail Server - Directory Traversal
| windows/remote/[01;31m[K21[m[K591.sh

ArGoSoft FTP Server 1.2.2.2 - Weak Password Encryption
| windows/remote/[01;31m[K21[m[K009.c

Arq 5.9.6 - Local Privilege Escalation
| macos/local/43[01;31m[K21[m[K8.sh

Arq 5.9.7 - Local Privilege Escalation
| macos/local/43[01;31m[K21[m[K6.rb

```
Art Gallery Management System Project v1.0 - Reflected Cross-Site
Scripting (XSS)                              |
php/webapps/51[01;31m[K21[m[K4.txt

Art Gallery Management System Project v1.0 - SQL Injection (cid)
Unauthenticated                              |
php/webapps/51[01;31m[K21[m[K5.txt

Art Gallery Management System Project v1.0 - SQL Injection (editid)
authenticated                                |
php/webapps/51[01;31m[K21[m[K6.txt

Artica Proxy 4.50 - Remote Code Execution (RCE)
| php/webapps/5[01;31m[K21[m[K46.py

Article Directory - 'index.php' Remote File Inclusion
| php/webapps/42[01;31m[K21[m[K.txt

Artifex MuPDF - Null Pointer Dereference
| linux/dos/4[01;31m[K21[m[K38.txt

Artifex MuPDF mujstest 1.10a - Null Pointer Dereference
| linux/dos/4[01;31m[K21[m[K39.txt

ArtiPHP 5.5.0 Neo - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                              |
php/webapps/37[01;31m[K21[m[K7.txt

aSc TimeTables 20[01;31m[K21[m[K.6.2 - Denial of Service (PoC)
| windows/local/49147.txt

ASCPU 0.60 Kernel - Memory File Descriptor Leakage
| unix/local/[01;31m[K21[m[K797.txt

askSam 4.0 Web Publisher - Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K435.txt

Asn Guestbook 1.5 - 'footer.php?version' Cross-Site Scripting
| php/webapps/260[01;31m[K21[m[K.txt

ASPBB 0.4 - 'topic.asp?TID' SQL Injection
| asp/webapps/268[01;31m[K21[m[K.txt

Aspee Ziyaretci Defteri - 'giris.asp' Multiple Field SQL Injections
| asp/webapps/29[01;31m[K21[m[K6.html

Asset Manager 1.0 - Arbitrary File Upload
| multiple/webapps/1[01;31m[K21[m[K33.txt

Asterisk PBX 0.7.x - Multiple Logging Format String Vulnerabilities
| linux/remote/242[01;31m[K21[m[K.pl
```

```
ASTPP VoIP Billing (4cf207a) - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K316.txt

Asx to Mp3 2.7.5 - Local Stack Overflow
| windows/local/349[01;31m[K21[m[K.pl

AT 3.1.8 - Formatted Time Heap Overflow
| linux/local/[01;31m[K21[m[K229.txt

Atar2b CMS 4.0.1 - 'gallery_e.php?id' SQL Injection
| php/webapps/365[01;31m[K21[m[K.txt

AtheOS 0.3.7 - Change Root Directory Escaping
| atheos/local/[01;31m[K21[m[K282.c

Atlassian Confluence 6.15.1 - Directory Traversal
| jsp/webapps/476[01;31m[K21[m[K.py

Atlassian JIRA FishEye 2.5.7 / Crucible 2.5.7 Plugins - XML Parsing
Security                                  |
jsp/webapps/372[01;31m[K21[m[K.txt

Atlassian Tempo 6.4.3 / JIRA 5.0.0 / Gliffy 3.7.0 - XML Parsing Denial
of Service                           | jsp/dos/37[01;31m[K21[m[K8.txt

AtomPhotoBlog 1.15 - 'atomPhotoBlog.php' SQL Injection
| php/webapps/3[01;31m[K21[m[K14.txt

ATP HTTPd 0.4 - Single Byte Buffer Overflow
| linux/remote/[01;31m[K21[m[K936.c

ATPhttpd 0.4b - Remote Buffer Overflow
| freebsd/remote/[01;31m[K21[m[K614.c

ATutor 1.2 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K21[m[K60.txt

Audio Editor Master 5.4.1.[01;31m[K21[m[K7 - Denial of Service
| windows/dos/19000.py

AudioPLUS 2.00.[01;31m[K21[m[K5 - '.lst' / '.m3u' Local Buffer Overflow
(SEH)                                          | windows/local/9064.pl

AudioPLUS 2.00.[01;31m[K21[m[K5 - '.m3u' / '.lst' Universal Overwrite
(SEH)                                           |
windows/local/9152.pl

AudioPLUS 2.00.[01;31m[K21[m[K5 - '.pls' Local Buffer Overflow (SEH)
| windows/local/9070.pl

AuroraGPT 4.0 - Remote Code Execution
| php/webapps/1[01;31m[K21[m[K55.txt
```

```
Authoria HR Suite - 'AthCGI.exe' Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K926.txt

Autodesk Backburner Manager 3 < 2016.0.0.[01;31m[K21[m[K50 - Null
Dereference Denial of Service                          |
windows/dos/41160.py

Autodesk Maya Script - Nodes Arbitrary Command Execution
| windows/local/10[01;31m[K21[m[K3.txt

Autodesk SoftImage Scene TOC - Arbitrary Command Execution
| windows/local/10[01;31m[K21[m[K1.txt

Automne.ws CMS 4.0.0rc2 - Multiple Remote File Inclusions
| php/webapps/104[01;31m[K21[m[K.txt

Auxilium PetRatePro - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K329.txt

Auxilium RateMyPet - Arbitrary File Upload (Metasploit)
| linux/webapps/[01;31m[K21[m[K836.rb

AV Arcade Free Edition - 'add_rating.php?id' Blind SQL Injection
| php/webapps/[01;31m[K21[m[K007.txt

Avast aswSnx.sys Kernel Driver 11.1.2253 - Memory Corruption Privilege
Escalation                          |
windows/dos/4[01;31m[K21[m[K82.cpp

Avaya IP Office (IPO) < 10.1 - 'SoftConsole' Remote Buffer Overflow
(SEH)                                    |
windows/remote/431[01;31m[K21[m[K.txt

Avaya IP Office Customer Call Reporter - 'ImageUpload.ashx' Remote
Command Execution (Metasploit)          |
windows/remote/[01;31m[K21[m[K847.rb

Avaya WinPMD UniteHostRouter - Remote Buffer Overflow (Metasploit)
| windows/remote/[01;31m[K21[m[K838.rb

AVE DOMINAplus 1.10.x - Cross-Site Request Forgery (enable/disable
alarm)                                    |
hardware/webapps/478[01;31m[K21[m[K.txt

Avira Antivirus 15.0.[01;31m[K21[m[K.86 - '.zip' Directory Traversal /
Command Execution                                  |
windows/local/40741.py

Ayman Akt IRCIT 0.3.1 - Invite Message Remote Buffer Overflow
| linux/dos/[01;31m[K21[m[K537.c

AzDGDatingLite 2.1.3 - Remote Code Execution
| php/webapps/1[01;31m[K21[m[K4.php
```

```
B2 0.6 - 'b2edit.showposts.php?b2inc' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K436.txt

Backdrop CMS 1.27.1 - Authenticated Remote Command Execution (RCE)
| php/webapps/520[01;31m[K21[m[K.py

Backup and Staging by WP Time Capsule 1.22.[01;31m[K21[m[K -
Unauthenticated Arbitrary File Upload                        |
php/webapps/5[01;31m[K21[m[K31.py

Baldr Botnet Panel - Arbitrary Code Execution (Metasploit)
| php/remote/47[01;31m[K21[m[K5.rb

BandSite CMS 1.1 - 'header.php' Cross-Site Scripting
| php/webapps/286[01;31m[K21[m[K.txt

Bandwebsite 1.5 - SQL Injection / Cross-Site Scripting
| php/webapps/7[01;31m[K21[m[K5.txt

Banex PHP MySQL Banner Exchange 2.[01;31m[K21[m[K - 'admin.php'
Multiple SQL Injections                                      |
php/webapps/28307.txt

Banex PHP MySQL Banner Exchange 2.[01;31m[K21[m[K -
'members.php?cfg_root' Remote File Inclusion                          |
php/webapps/28308.txt

Banex PHP MySQL Banner Exchange 2.[01;31m[K21[m[K -
'signup.php?site_name' SQL Injection                                  |
php/webapps/28306.txt

BanPro Dms 1.0 - 'index.php' Local File Inclusion
| php/webapps/31[01;31m[K21[m[K7.txt

Barracuda Networks Spam & Virus Firewall 4.1.1.0[01;31m[K21[m[K -
Remote Configuration Retrieval                          |
cgi/webapps/15130.sh

Barracuda Spam Firewall 3.3.03.053 - Remote Code Execution (1)
| hardware/remote/[01;31m[K21[m[K36.txt

Barracuda Spam Firewall 3.3.03.053 - Remote Code Execution (2)
| hardware/remote/[01;31m[K21[m[K45.txt

Barracuda Spam Firewall 3.3.x - 'preview_email.cgi?file' Arbitrary File
Access                            | cgi/webapps/283[01;31m[K21[m[K.pl

Base64 Decoder 1.1.2 - Local Buffer Overflow (SEH)
| windows/local/460[01;31m[K21[m[K.py

Basic Analysis and Security Engine (BASE) 1.4.5 -
'/setup/base_conf_contents.php' Multiple Remote File Inc |
php/webapps/367[01;31m[K21[m[K.txt
```

BasiliX Webmail 1.1 - Message Content Script Injection
| php/webapps/[01;31m[K21[m[K570.txt

Battle.net Clan Script 1.5.x - 'index.php' Multiple SQL Injections
| php/webapps/3[01;31m[K21[m[K81.txt

Battlefield 2/[01;31m[K21[m[K42 - Packet Null Pointer Dereference
Remote Denial of Service |
multiple/dos/35369.txt

BBC Education Betsie 1.5 - Parserl.pl Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K587.txt

bbPress 1.0.2 - Cross-Site Request Forgery (Change Admin Password)
| php/webapps/14[01;31m[K21[m[K4.txt

BBSXP CMS - Multiple SQL Injections
| asp/webapps/371[01;31m[K21[m[K.txt

BbZL.php 0.92 - Insecure Cookie Handling
| php/webapps/66[01;31m[K21[m[K.txt

BEA Systems WebLogic Server and Express 7.0 - Null Character Denial of
Service |
windows/dos/[01;31m[K21[m[K432.txt

Beerwin's PHPLinkAdmin 1.0 - Remote File Inclusion / SQL Injection
| php/webapps/8[01;31m[K21[m[K6.txt

Beetel BCM96338 Router - DNS Change
| hardware/webapps/4[01;31m[K21[m[K96.sh

Behold! Software Web Page Counter 2.7 - Denial of Service
| multiple/dos/19[01;31m[K21[m[K2.txt

Belkin F5D6130 Wireless Network Access Point - SNMP Request Denial of
Service |
hardware/dos/[01;31m[K21[m[K756.txt

Ben Chivers Easy Guestbook 1.0 - Administrative Access
| cgi/webapps/[01;31m[K21[m[K659.html

Ben Chivers Easy Homepage Creator 1.0 - File Modification
| cgi/webapps/[01;31m[K21[m[K658.html

Benjamin Lefevre Dobermann Forum 0.x - 'entete.php?subpath' Remote File
Inclusion | php/webapps/[01;31m[K21[m[K967.txt

Benjamin Lefevre Dobermann Forum 0.x - 'enteteacceuil.php?subpath'
Remote File Inclusion |
php/webapps/[01;31m[K21[m[K968.txt

```
Benjamin Lefevre Dobermann Forum 0.x - 'index.php?subpath' Remote File
Inclusion                              |
php/webapps/[01;31m[K21[m[K969.txt

Benjamin Lefevre Dobermann Forum 0.x - 'newtopic.php?subpath' Remote
File Inclusion                         |
php/webapps/[01;31m[K21[m[K970.txt

bfcommand & control server 1.22/2.0/2.14 manager - Multiple
Vulnerabilities                                  |
multiple/remote/26[01;31m[K21[m[K0.txt

bharat Mediratta Gallery 1.1/1.2 - Directory Traversal
| php/webapps/[01;31m[K21[m[K157.txt

Bharat Mediratta Gallery 1.x - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K676.txt

BibORB 1.3.2 Login Module - Multiple SQL Injections
| php/webapps/251[01;31m[K21[m[K.txt

BigPond 3G[01;31m[K21[m[KWB - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K21[m[K992.txt

BigTree CMS 4.2.3 - (Authenticated) SQL Injection
| php/webapps/378[01;31m[K21[m[K.txt

Bild Flirt System 1.0 - SQL Injection
| php/webapps/122[01;31m[K21[m[K.rb

BIND - 'TSIG' Denial of Service
| multiple/dos/485[01;31m[K21[m[K.py

BIND 9.10.5 - Unquoted Service Path Privilege Escalation
| windows/local/4[01;31m[K21[m[K[01;31m[K21[m[K.txt

binutils 2.29.51.201709[01;31m[K21[m[K - 'read_1_byte' Heap Buffer
Overflow                                                |
linux/dos/42970.txt

BisonWare BisohFTP Server 3.5 - Multiple Vulnerabilities
| linux/remote/19[01;31m[K21[m[K9.c

BitchX 1.1 Final - MODE Remote Heap Overflow
| linux/remote/43[01;31m[K21[m[K.rb

BitMover BitKeeper 3.0 - Daemon Mode Remote Command Execution
| multiple/remote/2[01;31m[K21[m[K45.txt

Bits Video Script 2.04/2.05 - 'search.php' Cross-Site Scripting
| php/webapps/341[01;31m[K21[m[K.txt
```

```
Bitweaver 2.8.1 - Multiple Vulnerabilities
| php/webapps/22[01;31m[K21[m[K6.txt

Bitweaver 2.8.1 - Persistent Cross-Site Scripting
| php/webapps/16[01;31m[K21[m[K7.txt

BL4 SMTP Server < 0.1.5 - Remote Buffer Overflow (PoC)
| windows/dos/17[01;31m[K21[m[K.pl

BlackBoard 5.0 - Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K588.txt

BlackMoon FTP Server 3.1.2.1731 - 'BMFTP-RELEASE' Unquoted Serive Path
| windows/local/475[01;31m[K21[m[K.txt

Blahz-DNS 0.2 - Direct Script Call Authentication Bypass
| php/webapps/[01;31m[K21[m[K426.txt

BlazeDVD 5.0 - '.PLF' Playlist File Remote Buffer Overflow
| windows/remote/6[01;31m[K21[m[K7.pl

BlazeVideo HDTV Player 3.5 - '.PLF' File Stack Buffer Overflow
| windows/remote/3[01;31m[K21[m[K29.cpp

Blazix 1.2 - Password Protected Directory Information Disclosure
| multiple/remote/[01;31m[K21[m[K752.txt

Blazix 1.2 - Special Character Handling Server Side Script Information
Disclosure                          |
multiple/remote/[01;31m[K21[m[K751.txt

Blitzkrieg 2 < 1.[01;31m[K21[m[K - 'Server/Client' Denial of Service
| windows/dos/1282.c

Blog Mod 0.1.9 - 'index.php?month' SQL Injection
| php/webapps/[01;31m[K21[m[K786.php

Blog System 1.5 - Multiple Vulnerabilities
| php/webapps/1[01;31m[K21[m[K92.txt

Blog System 1.x - 'note' SQL Injection
| php/webapps/11[01;31m[K21[m[K6.txt

BlueFace Falcon Web Server 2.0 - Error Message Cross-Site Scripting
| windows/remote/[01;31m[K21[m[K698.txt

BlueSocket BSC [01;31m[K21[m[K00 5.0/5.1 - Admin.pl Cross-Site
Scripting                                                  |
cgi/webapps/292[01;31m[K21[m[K.txt

BOA Web Server 0.94.14rc[01;31m[K21[m[K - Arbitrary File Access
| linux/webapps/42290.txt
```

Boite de News 4.0.1 - 'index.php' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K53.txt

Booking Calendar - Multiple Vulnerabilities
| php/webapps/314[01;31m[K21[m[K.txt

BOOTP Turbo 2.0.1[01;31m[K21[m[K4 - 'BOOTP Turbo' Unquoted Service Path
| windows/local/48078.txt

Boozt 0.9.8 - Remote Buffer Overflow
| linux/remote/[01;31m[K21[m[K205.c

Borland Interbase 2007/2007 SP2 - 'INET_connect' Remote Buffer Overflow
(Metasploit) | linux/remote/100[01;31m[K21[m[K.rb

boxalino 09.05.25-04[01;31m[K21[m[K - Directory Traversal
| multiple/webapps/9872.txt

BPM Studio Pro 4.2 - HTTPd Directory Traversal
| windows/remote/[01;31m[K21[m[K311.txt

Brian Dorricott MAILTO 1.0.7-9 - Unauthorized Mail Server Use
| windows/remote/[01;31m[K21[m[K178.html

Broadcom PIPA C[01;31m[K21[m[K1 - Sensitive Information Disclosure
| hardware/webapps/33353.txt

Broadlight Residential Gateway DI3124 - Remote DNS Change
| hardware/webapps/37[01;31m[K21[m[K4.txt

Browse3D 3.5 - '.sfs' Local Buffer Overflow (PoC)
| windows/dos/77[01;31m[K21[m[K.pl

BrowseFTP Client 1.62 - Remote Buffer Overflow
| windows/remote/[01;31m[K21[m[K201.pl

BRS Webweaver 1.0 1 - MKDir Directory Traversal
| linux/remote/2[01;31m[K21[m[K43.txt

BRU 17.0 - SetLicense Script Insecure Temporary File Symbolic Link
| linux/local/[01;31m[K21[m[K247.c

BRU 17.0 - XBRU Insecure Temporary File
| linux/local/[01;31m[K21[m[K793.txt

BSCW 3.4/4.0 - Insecure Default Installation
| multiple/remote/[01;31m[K21[m[K197.txt

BSD / Linux - 'umount' Local Privilege Escalation
| multiple/local/3[01;31m[K21[m[K.c

BSDI 3.0/3.1 - Local Kernel Denial of Service
| bsd/dos/[01;31m[K21[m[K077.c

```
BSI Advance Hotel Booking System 2.0 - 'booking_details.php Persistent
Cross-Site Scripting                |
php/webapps/47[01;31m[K21[m[K9.txt

BubbleMon 1.x Kernel - Memory File Descriptor Leakage
| unix/local/[01;31m[K21[m[K796.txt

BugHunter HTTP Server 1.6.2 - Parse Error Information Disclosure
| multiple/remote/30[01;31m[K21[m[K8.txt

Build Smart ERP [01;31m[K21[m[K.0817 - 'eidValue' SQL Injection
(Unauthenticated)                                    |
asp/webapps/50445.txt

Burning Board 1.1.1 - 'URL' Manipulation
| php/webapps/[01;31m[K21[m[K380.php

BuzzyWall 1.3.2 - 'resolute.php' Information Disclosure
| php/webapps/36[01;31m[K21[m[K4.txt

bwired - 'index.php?newsID' SQL Injection
| php/webapps/4[01;31m[K21[m[K3.txt

C.P.Sub 4.5 - Authentication Bypass
| php/webapps/265[01;31m[K21[m[K.py

C/C++ Offline Compiler and C For OS - Persistent Cross-Site Scripting
| ios/webapps/397[01;31m[K21[m[K.txt

CA BrightStor ARCserve - 'msgeng.exe' Remote Heap Overflow (1)
| windows/remote/3[01;31m[K21[m[K1.py

CA BrightStor ARCserve - 'msgeng.exe' Remote Heap Overflow (2)
| windows/remote/3[01;31m[K21[m[K8.pl

Cacheflow CacheOS 3.1.x/4.0.x/4.1 - Unresolved Domain Cross-Site
Scripting                                |
multiple/remote/[01;31m[K21[m[K649.txt

Cacheflow CacheOS 3.1/4.0 Web Administration - Arbitrary Cached Page
Code Leakage                           |
multiple/remote/[01;31m[K21[m[K[01;31m[K21[m[K2.txt

Cag CMS 0.2 - Cross-Site Scripting / Blind SQL Injection
| php/webapps/15[01;31m[K21[m[K0.txt

calacode @mail webmail system 3.52 - Multiple Vulnerabilities
| cgi/webapps/234[01;31m[K21[m[K.txt

Caldera OpenServer 5.0.5/5.0.6 - SCOAdmin Symbolic Link
| sco/local/[01;31m[K21[m[K489.txt
```

```
Caldera OpenServer 5.0.x - XSCO Color Database File Heap Overflow
| unix/dos/[01;31m[K21[m[K531.txt

Caldera OpenUnix 8.0/UnixWare 7.1.1 / HP HP-UX 11.0 / Solaris 7.0 /
SunOS 4.1.4 - rpc.cmsd Buffer Overflow |
multiple/remote/194[01;31m[K21[m[K.c

Caldera UnixWare 7.1.1 - Message Catalog Environment Variable Format
String                                  |
unixware/local/[01;31m[K21[m[K284.c

Caldera UnixWare 7.1.1 - WebTop 'SCOAdminReg.cgi' Arbitrary Command
Execution                               |
unixware/local/[01;31m[K21[m[K239.sh

Caldera X Server 7.1/8.0 - External Program Privileged Invocation
| unix/local/[01;31m[K21[m[K758.txt

Calibre-web 0.6.[01;31m[K21[m[K - Stored XSS
| multiple/webapps/52067.txt

Campaign Enterprise 11.0.4[01;31m[K21[m[K - SQL Injection
| multiple/webapps/18430.txt

CANDID - '/image/view.php?image_id' SQL Injection
| php/webapps/34[01;31m[K21[m[K9.txt

Cannonbolt Portfolio Manager 1.0 - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K132.txt

Canon PRINT 2.5.5 - Information Disclosure
| android/local/473[01;31m[K21[m[K.txt

Captaris Infinite WebMail 3.61.5 - HTML Injection
| php/webapps/2[01;31m[K21[m[K04.txt

Cartweaver 3 - Local File Inclusion
| php/webapps/[01;31m[K21[m[K989.txt

CartWIZ 1.10 - 'searchresults.asp' SKU Argument Cross-Site Scripting
| asp/webapps/255[01;31m[K21[m[K.txt

Cat Soft Serv-U FTP Server 2.5 - Remote Buffer Overflow
| linux/remote/19[01;31m[K21[m[K8.c

CatDV 9.2 - RMI Authentication Bypass
| java/remote/496[01;31m[K21[m[K.java

cattaDoc 2.[01;31m[K21[m[K - 'download2.php?fn1' Remote File Disclosure
| php/webapps/3677.txt

CCProxy 6.2 - 'ping' Remote Buffer Overflow
| windows/remote/6[01;31m[K21[m[K.py
```

CDRDAO 1.1.x - Home Directory Configuration File Symbolic Link (1)
| linux/local/[01;31m[K21[m[K[01;31m[K21[m[K6.sh

CDRDAO 1.1.x - Home Directory Configuration File Symbolic Link (2)
| linux/local/[01;31m[K21[m[K[01;31m[K21[m[K7.sh

CDRDAO 1.1.x - Home Directory Configuration File Symbolic Link (3)
| linux/local/[01;31m[K21[m[K[01;31m[K21[m[K8.sh

CDRDAO 1.1.x - Home Directory Configuration File Symbolic Link (4)
| linux/local/[01;31m[K21[m[K[01;31m[K21[m[K9.sh

Cela Link CLR-M20 2.7.1.6 - Arbitrary File Upload
| hardware/webapps/450[01;31m[K21[m[K.txt

Cemu 1.6.4b - Information Leak / Buffer Overflow (Emulator Breakout)
| multiple/local/410[01;31m[K21[m[K.md

Centos WebPanel 7 - 'term' SQL Injection
| linux/webapps/48[01;31m[K21[m[K2.txt

Centrinity FirstClass Desktop Client 7.1 - Local Buffer Overflow
| windows/local/239[01;31m[K21[m[K.c

Centron 19.04 - Remote Code Execution (RCE)
| php/webapps/5[01;31m[K21[m[K56.py

Century Software Term For Linux 6.27.869 - Command Line Buffer Overflow
| linux/local/[01;31m[K21[m[K302.c

CEWE Photoshow 6.3.4 - Denial of Service (PoC)
| windows_x86-64/dos/45[01;31m[K21[m[K1.py

CGIEmail 1.6 - Remote Buffer Overflow
| linux/remote/[01;31m[K21[m[K998.c

CGIScript.net - 'csPassword.cgi' 1.0 HTAccess File Modification
| cgi/webapps/[01;31m[K21[m[K495.txt

CGIScript.net - 'csPassword.cgi' 1.0 Information Disclosure
| cgi/webapps/[01;31m[K21[m[K494.txt

CGIScript.net - csMailto Hidden Form Field Remote Command Execution
| cgi/remote/[01;31m[K21[m[K415.txt

CGIScript.net 1.0 - Information Disclosure
| cgi/webapps/[01;31m[K21[m[K460.pl

CGIScript.net csNews 1.0 - Double URL Encoding Unauthorized
Administrative Access |
cgi/webapps/[01;31m[K21[m[K532.txt

CGIScript.net csNews 1.0 - Header File Type Restriction Bypass
| cgi/webapps/[01;31m[K21[m[K533.txt

CGIWrap 2.x/3.x - Cross-Site Scripting
| cgi/remote/[01;31m[K21[m[K023.txt

Charity Management System CMS 1.0 - Multiple Vulnerabilities
| php/webapps/50[01;31m[K21[m[K7.txt

Chaussette 080706 - '_BASE' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K69.txt

Check Point Endpoint Security - Full Disk Encryption RDP Connection
Denial of Service |
hardware/dos/33[01;31m[K21[m[K6.txt

Check Point Firewall-1 4 Securemote - Network Information Leak
| hardware/remote/[01;31m[K21[m[K015.pl

Check Point Software Firewall-1 3.0/1 4.0 - Session Agent Impersonation
| windows/remote/20[01;31m[K21[m[K4.pl

Check Point Software Firewall-1 3.0/1 4.0/1 4.1 - Session Agent
Dictionary Attack (1) |
multiple/remote/20[01;31m[K21[m[K5.pl

Check Point Software Firewall-1 3.0/1 4.0/1 4.1 - Session Agent
Dictionary Attack (2) |
multiple/remote/20[01;31m[K21[m[K6.sh

Check_MK 1.2.8p25 - Information Disclosure
| python/webapps/430[01;31m[K21[m[K.py

chernobiLe Portal 1.0 - 'default.asp' SQL Injection
| asp/webapps/3[01;31m[K21[m[K0.txt

CHETCPASSWD 1.12 - Shadow File Disclosure
| cgi/webapps/2[01;31m[K21[m[K11.pl

Chinput 3.0 - Environment Variable Buffer Overflow
| linux/local/[01;31m[K21[m[K231.c

Chromacam 4.0.3.0 - PsyFrameGrabberService Unquoted Service Path
| windows/local/51[01;31m[K21[m[K0.txt

Chupix CMS Contact Module 0.1 - 'index.php' Multiple Local File
Inclusions |
php/webapps/3[01;31m[K21[m[K80.txt

ChurchCRM 5.9.1 - SQL Injection
| php/webapps/5[01;31m[K21[m[K52.NA

ChurchCRM v4.5.3-1[01;31m[K21[m[Kfcc1 - SQL Injection
| php/webapps/51296.txt

Cimetrics BACnet Explorer 4.0 - XML External Entity Injection
| windows/local/413[01;31m[K21[m[K.txt

Cisco AS5350 - Universal Gateway Portscan Denial of Service
| hardware/dos/[01;31m[K21[m[K971.txt

Cisco ATA-186 - HTTP Device Configuration Disclosure
| hardware/remote/[01;31m[K21[m[K441.txt

Cisco Catalyst 2960 IOS 12.2(55)SE1 - 'ROCEM' Remote Code Execution
| hardware/remote/4[01;31m[K21[m[K22.py

Cisco CatOS 5.x/6.1/7.3/7.4 - CiscoView HTTP Server Buffer Overflow
| hardware/remote/[01;31m[K21[m[K944.pl

Cisco CBOS 2.x - Broadband Operating System TCP/IP Stack Denial of
Service |
hardware/dos/[01;31m[K21[m[K472.pl

Cisco CBOS 2.x - Multiple TCP Connection Denial of Service
Vulnerabilities |
hardware/dos/[01;31m[K21[m[K092.txt

Cisco DPC[01;31m[K21[m[K00 - Denial of Service
| hardware/dos/[01;31m[K21[m[K523.txt

Cisco DPC[01;31m[K21[m[K00 2.0.2 r1256-060303 - Multiple Security
Bypass / Cross-Site Request Forgery Vulnerabilities |
hardware/remote/34033.html

Cisco HSRP - Denial of Service
| hardware/dos/208[01;31m[K21[m[K.txt

Cisco IDS Device Manager 3.1.1 - Arbitrary File Read Access
| hardware/remote/[01;31m[K21[m[K456.txt

Cisco IOS 11.x - TFTP Server Long File Name Buffer Overflow
| hardware/dos/[01;31m[K21[m[K655.c

Cisco IOS 11.x/12.0 - ICMP Redirect Denial of Service
| hardware/dos/[01;31m[K21[m[K465.txt

Cisco IOS 11/12 - SNMP Message Denial of Service
| hardware/dos/[01;31m[K21[m[K296.c

Cisco IOS 12 - UDP Denial of Service
| hardware/dos/[01;31m[K21[m[K028.pl

Cisco LEAP - Password Disclosure
| hardware/remote/23[01;31m[K21[m[K2.txt

Cisco RV110W/RV130(W)/RV[01;31m[K21[m[K5W Routers Management Interface - Remote Command Execution (Metasploit) | hardware/remote/47348.rb

Cisco Secure ACS for Windows NT 3.0 - Cross-Site Scripting | windows/remote/[01;31m[K21[m[K555.txt

Cisco Secure IDS 2.0/3.0 / Snort 1.x / ISS RealSecure 5/6 / NFR 5.0 - Encoded IIS Detection Evasion | multiple/remote/[01;31m[K21[m[K100.pl

Cisco Smart Software Manager On-Prem 8-202206 - Account Takeover | multiple/webapps/5[01;31m[K21[m[K55.py

Cisco VPN 3000 Series Concentrator Client - Authentication Denial of Service | hardware/dos/[01;31m[K21[m[K770.c

Cisco VPN 5000 Client - Buffer Overrun (1) | unix/local/[01;31m[K21[m[K805.c

Cisco VPN 5000 Client - Buffer Overrun (2) | unix/local/[01;31m[K21[m[K806.c

Cisco VPN Client for Unix 3.5.1 - Local Buffer Overflow | linux/local/[01;31m[K21[m[K568.c

Citrix Metaframe 1.0/1.8 - Weak Encryption | multiple/local/198[01;31m[K21[m[K.c

Citrix Metaframe for Windows NT 4.0 TSE 1.8 - Java ICA Environment Denial of Service | windows/dos/[01;31m[K21[m[K703.txt

Citrix NFuse 1.51/1.6 - Cross-Site Scripting | jsp/remote/[01;31m[K21[m[K355.txt

Citrix Nfuse 1.6 - Published Applications Information Leak | windows/remote/[01;31m[K21[m[K235.pl

Citrix Published Applications - Information Disclosure | windows/remote/[01;31m[K21[m[K913.txt

CKEditor 3 - Server-Side Request Forgery (SSRF) | php/webapps/500[01;31m[K21[m[K.txt

ClanSphere 2011.3 - 'cs_lang' Cookie Local File Inclusion | php/webapps/2[01;31m[K21[m[K81.txt

Claroline 1.8 - '/tracking/courseLog.php?view' Cross-Site Scripting | php/webapps/3[01;31m[K21[m[K08.txt

```
Claroline 1.8 - '/tracking/toolaccess_details.php?toolId' Cross-Site
Scripting                              |
php/webapps/3[01;31m[K21[m[K09.txt

Claroline 1.8 - 'learnPath/calendar/myagenda.php' Query String Cross-
Site Scripting                         |
php/webapps/3[01;31m[K21[m[K06.txt

Claroline 1.8 - 'user/user.php' Query String Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K07.txt

Clever Copy 3.0 - 'Connect.INC' Information Disclosure
| php/webapps/276[01;31m[K21[m[K.txt

Clever Database Comparer ActiveX 2.2 - Remote Buffer Overflow (PoC)
| windows/dos/39[01;31m[K21[m[K.html

Clicky Web Pseudo-frames 1.0 - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K454.txt

ClipSharePro 4.1 - Local File Inclusion
| php/webapps/3[01;31m[K21[m[K31.txt

Clipster Video - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K133.txt

Clix'N'Cash Clone 2010 - 'index.php' SQL Injection
| php/webapps/34[01;31m[K21[m[K7.txt

CloudMe Sync 1.11.2 - Buffer Overflow + Egghunt
| windows/remote/46[01;31m[K21[m[K8.py

CLUB-Nuke [XP] 2.0 LCID 2048 (Turkish Version) - SQL Injection
| asp/webapps/[01;31m[K21[m[K50.txt

CMS Made Simple 0.10 - 'Lang.php' Remote File Inclusion
| php/webapps/26[01;31m[K21[m[K7.html

cmsphp 0.[01;31m[K21[m[K - Local File Inclusion / Cross-Site Scripting
| php/webapps/9311.txt

cmsWorks 2.2 RC4 - 'mod_root' Remote File Inclusion
| php/webapps/59[01;31m[K21[m[K.txt

CMU CERT/CC VINCE 2.0.6 - Stored XSS
| multiple/webapps/5[01;31m[K21[m[K81.txt

Cobalt Linux 6.0 - RaQ (Authenticated) Privilege Escalation
| unix/local/[01;31m[K21[m[K790.sh

Cobalt Qube 3.0 - Authentication Bypass
| php/webapps/[01;31m[K21[m[K640.txt
```

```
Cobalt RaQ 2.0/3.0/4.0 XTR - 'MultiFileUpload.php' Authentication
Bypass (1)                                  |
php/remote/[01;31m[K21[m[K334.pl

Cobalt RaQ 2.0/3.0/4.0 XTR - 'MultiFileUpload.php' Authentication
Bypass (2)                                  |
php/remote/[01;31m[K21[m[K335.sh

CodeAstro Online Railway Reservation System 1.0 - Cross Site Scripting
(XSS)                                  |
php/webapps/5[01;31m[K21[m[K59.txt

CodeBlue 5.1 - SMTP Response Buffer Overflow
| windows/remote/[01;31m[K21[m[K643.c

CodeCanyon RISE CRM 3.7.0 - SQL Injection
| php/webapps/5[01;31m[K21[m[K00.py

CodeIgniter 2.1 - 'xss_clean()' Filter Security Bypass
| php/webapps/375[01;31m[K21[m[K.txt

ColdFusion MX - Missing Template Cross-Site Scripting
| cfm/remote/[01;31m[K21[m[K548.txt

Combat Evolved 1.0.7.0615 - Multiple Denial of Service Vulnerabilities
| multiple/dos/3[01;31m[K21[m[K92.txt

COMMAX CVD-Axx DVR 5.1.4 - Weak Default Credentials Stream Disclosure
| hardware/webapps/50[01;31m[K21[m[K0.txt

common Solutions csphonebook 1.02 - 'index.php' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K35.txt

Comodo GeekBuddy < 4.18.1[01;31m[K21[m[K - Local Privilege Escalation
| windows/local/37065.txt

Company's Recruitment Management System 1.0. - 'title' Stored Cross-
Site Scripting (XSS)                    |
php/webapps/504[01;31m[K21[m[K.txt

Compaq Client Management Agents 3.70/4.0 / Insight Management Agents
4.[01;31m[K21[m[K A/4.22 A/4.30 A / Intelligent Cl |
multiple/dos/19225.txt

CompleteFTP 3.3.0 - Remote Memory Consumption Denial of Service
| windows/dos/1[01;31m[K21[m[K10.pl

Conceptronic Grab'n'Go Network Storage - Directory Traversal
| hardware/webapps/[01;31m[K21[m[K032.txt

Concrete CMS < 5.5.[01;31m[K21[m[K - Multiple Vulnerabilities
| php/webapps/37225.pl
```

```
Concrete5 8.5.4 - 'name' Stored XSS
| php/webapps/497[01;31m[K21[m[K.txt

Confixx Pro 3.3.1 - 'saveserver.php' Remote File Inclusion
| php/webapps/4[01;31m[K21[m[K9.txt

COOL! Remote Control 1.12 - Remote Denial of Service
| windows/dos/1[01;31m[K21[m[K2.pl

Cooolsoft PowerFTP Server 2.0 3/2.10 - Multiple Denial of Service
Vulnerabilities (1)                       |
windows/dos/[01;31m[K21[m[K162.pl

Cooolsoft PowerFTP Server 2.0 3/2.10 - Multiple Denial of Service
Vulnerabilities (2)                       |
windows/dos/[01;31m[K21[m[K163.pl

Cooolsoft PowerFTP Server 2.x - Remote Denial of Service (1)
| windows/dos/[01;31m[K21[m[K907.c

Cooolsoft PowerFTP Server 2.x - Remote Denial of Service (2)
| windows/dos/[01;31m[K21[m[K908.pl

Cooolsoft PowerFTP Server 2.x - Remote Denial of Service (3)
| windows/dos/[01;31m[K21[m[K909.txt

Coppermine Photo Gallery 1.4.[01;31m[K21[m[K - 'css' Cross-Site
Scripting                                                 |
php/webapps/32963.txt

CorelDRAW X7 CDR File - 'CdrTxt.dll' Off-by-One Stack Corruption
| windows/dos/35[01;31m[K21[m[K7.txt

CosCMS 1.7[01;31m[K21[m[K - OS Command Injection
| php/webapps/24629.txt

Cosy+ firmware [01;31m[K21[m[K.2s7 - Command Injection
| multiple/hardware/5[01;31m[K21[m[K60.py

COVID19 Testing Management System 1.0 - 'Multiple' SQL Injections
| php/webapps/50[01;31m[K21[m[K5.txt

cPanel - HTTP Response Splitting
| multiple/webapps/11[01;31m[K21[m[K1.txt

cPanel 11.18.3/11.[01;31m[K21[m[K - 'manpage.html' Cross-Site Scripting
| php/webapps/31472.txt

cPanel 11.[01;31m[K21[m[K - 'wwwact' Privilege Escalation
| php/webapps/31807.txt

Craft CMS 2.6 - Cross-Site Scripting
| php/webapps/4[01;31m[K21[m[K43.txt
```

Crafty Syntax Live Help 2.14.6 - 'livehelp_js.php' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K69.txt

Creston Web Interface 1.0.0.[01;31m[K21[m[K59 - Credential Disclosure
| hardware/webapps/50675.txt

Crime records Management System 1.0 - 'Multiple' SQL Injection
(Authenticated) |
php/webapps/50[01;31m[K21[m[K3.txt

Critical Path InJoin Directory Server 4.0 - Cross-Site Scripting
| multiple/remote/[01;31m[K21[m[K444.txt

Critical Path InJoin Directory Server 4.0 - File Disclosure
| multiple/remote/[01;31m[K21[m[K445.txt

crossfire-server 1.9.0 - 'SetUp()' Remote Buffer Overflow
| linux/remote/50[01;31m[K21[m[K6.py

Cryptocat 2.0.[01;31m[K21[m[K Chrome Extension - 'img/keygen.gif' File
Information Disclosure |
multiple/remote/38636.txt

Crysis 1.[01;31m[K21[m[K - 'keyexchange' Packet Information Disclosure
| multiple/remote/31918.txt

Crysis 1.[01;31m[K21[m[K - HTTP/XML-RPC Service Remote Denial of
Service |
multiple/dos/31931.txt

Crysis 1.[01;31m[K21[m[K/1.5 - HTTP/XML-RPC Service Access Violation
Remote Denial of Service |
multiple/dos/33096.txt

CSO Lanifex Outreach Project Tool 0.946b - Request Origin Spoofing
| multiple/remote/2[01;31m[K21[m[K79.pl

CSSearch 2.3 - Remote Command Execution
| cgi/remote/[01;31m[K21[m[K354.txt

CubeCart 3.0.11 - 'oid' Blind SQL Injection
| php/webapps/[01;31m[K21[m[K98.php

CUPS 1.1.x - Negative Length HTTP Header
| linux/remote/2[01;31m[K21[m[K06.txt

CuteCast 1.2 - User Credential Disclosure
| cgi/webapps/[01;31m[K21[m[K995.txt

CuteFTP 4.2 - Default Weak Password Encoding
| windows/local/[01;31m[K21[m[K090.txt

```
CuteNews 1.3.6 - 'result' Cross-Site Scripting
| php/webapps/29[01;31m[K21[m[K7.txt

CuteNews 1.4.0 - Shell Injection / Remote Command Execution
| php/webapps/12[01;31m[K21[m[K.php

CVS 1.11.x - Directory Request Double-Free Heap Corruption
| linux/remote/2[01;31m[K21[m[K87.txt

Cwfm 0.9.1 - 'Language' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K51.txt

CyberPanel 2.3.6 - Remote Code Execution (RCE)
| multiple/webapps/5[01;31m[K21[m[K72.py

Cyberstop Web Server 0.1 - Long Request Denial of Service
| windows/dos/[01;31m[K21[m[K237.pl

CyBoards PHP Lite 1.[01;31m[K21[m[K - 'script_path' Remote File
Inclusion                                                 |
php/webapps/3660.pl

CyBoards PHP Lite 1.[01;31m[K21[m[K/1.25 - 'Common.php' Remote File
Inclusion                                              |
php/webapps/27970.txt

CyBoards PHP Lite 1.[01;31m[K21[m[K/1.25 - 'post.php' SQL Injection
| php/webapps/27422.txt

Cyme ChartFX Client Server - ActiveX Control Array Indexing
| windows/dos/[01;31m[K21[m[K737.txt

Cyphor 0.19 - 'show.php?id' SQL Injection
| php/webapps/13[01;31m[K21[m[K.pl

Cyrus IMAPD 2.3.2 - 'pop3d' Remote Buffer Overflow (3)
| linux/remote/[01;31m[K21[m[K85.pl

D-Link DIR-600M Wireless - Cross-Site Scripting
| hardware/webapps/44[01;31m[K21[m[K9.txt

D-Link DIR-615 - Cross-Site Request Forgery
| hardware/webapps/418[01;31m[K21[m[K.txt

D-Link DIR-815 - Multiple Vulnerabilities
| hardware/remote/387[01;31m[K21[m[K.txt

D-Link Dl-704 2.56 b5 - IP Fragment Denial of Service
| hardware/dos/[01;31m[K21[m[K103.c

D-Link DSL-2640B ADSL Router - 'dnscfg' Remote DNS Change
| hardware/webapps/4[01;31m[K21[m[K97.sh
```

D-Link DSL-2640U - DNS Change
| hardware/webapps/4[01;31m[K21[m[K95.sh

D3DGear 5.00 Build [01;31m[K21[m[K75 - Buffer Overflow (PoC)
| windows/dos/43410.py

DaCode 1.2 - News Message HTML Injection
| php/webapps/[01;31m[K21[m[K861.txt

Daily Expense Manager 1.0 - Cross-Site Request Forgery (Delete Income)
| php/webapps/47[01;31m[K21[m[K3.txt

Dasan Networks GPON ONT WiFi Router H640X 12.02-011[01;31m[K21[m[K /
2.77p1-1124 / 3.03p2-1146 - Remote Code Execution |
hardware/webapps/44074.md

Dasan Networks GPON ONT WiFi Router H64X Series - Cross-Site Request
Forgery |
hardware/webapps/423[01;31m[K21[m[K.txt

DataEase 2.4.0 - Database Configuration Information Exposure
| java/webapps/5[01;31m[K21[m[K28.py

DB4Web 3.4/3.6 - Connection Proxy
| multiple/remote/[01;31m[K21[m[K801.txt

DB4Web 3.4/3.6 - File Disclosure
| multiple/remote/[01;31m[K21[m[K800.txt

DBHcms 1.1.4 - 'dbhcms_user/SearchString' SQL Injection
| php/webapps/153[01;31m[K21[m[K.txt

DC/OS Marathon UI - Docker (Metasploit)
| python/remote/4[01;31m[K21[m[K34.rb

DCP-Portal 5.0.1 - 'editor.php?Root' Remote File Inclusion
| php/webapps/2[01;31m[K21[m[K26.txt

DCP-Portal 5.0.1 - 'lib.php?Root' Remote File Inclusion
| php/webapps/2[01;31m[K21[m[K27.txt

DCShop Beta 1.0 - Form Manipulation
| cgi/webapps/[01;31m[K21[m[K352.txt

DD-WRT - Site Survey SSID Script Injection
| multiple/remote/3[01;31m[K21[m[K89.py

Debian bsdmainutils 6.0.14 - Calendar Information Disclosure
| linux/local/244[01;31m[K21[m[K.c

DeleGate 7.7.1 - Cross-Site Scripting
| multiple/remote/[01;31m[K21[m[K193.txt

```
Dell EMC RecoverPoint < 5.1.2 - Remote Root Command Execution
| linux/remote/449[01;31m[K21[m[K.txt

Dell Webcam Software Bundled - ActiveX Remote Buffer Overflow
| windows/remote/186[01;31m[K21[m[K.txt

DELTAScripts PHP Classifieds 6.20 - 'Member_Login.php' SQL Injection
| php/webapps/27[01;31m[K21[m[K4.txt

Demarc PureSecure 1.0.5 - Authentication Check SQL Injection
| multiple/remote/[01;31m[K21[m[K384.txt

Denicomp Winsock RSHD/NT Standard Error 2.20.00 - Denial of Service
| windows/dos/[01;31m[K21[m[K174.c

Denicomp Winsock RSHD/NT Standard Error 2.[01;31m[K21[m[K.00 - Denial
of Service                                          |
windows/dos/[01;31m[K21[m[K175.c

Destiny Media Player 1.61 - '.pls' Universal Buffer Overflow (SEH)
| windows/local/93[01;31m[K21[m[K.pl

DEV Web Management System 1.5 - Multiple Input Validation
Vulnerabilities                                     |
php/webapps/3[01;31m[K21[m[K30.txt

Device Monitoring Studio 8.10.00.8925 - Denial of Service (PoC)
| windows/dos/463[01;31m[K21[m[K.py

DHCP Server 2.5.2 - Denial of Service (PoC)
| windows/dos/467[01;31m[K21[m[K.py

Digital Unix 4.0 - MSGCHK Buffer Overflow
| unix/local/[01;31m[K21[m[K105.c

Digital Unix 4.0 - MSGCHK MH_PROFILE Symbolic Link
| unix/local/[01;31m[K21[m[K107.sh

DigitalPersona 4.5.0.2[01;31m[K21[m[K3 - 'DpHostW' Unquoted Service
Path                                                |
windows/local/49008.txt

Discloser 0.0.4 - 'fileloc' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K88.txt

DiscusWare Discus 3.10 - Error Message Cross-Site Scripting
| cgi/webapps/270[01;31m[K21[m[K.txt

Discuz! 6.0.1 - 'searchid' SQL Injection
| php/webapps/6[01;31m[K21[m[K4.php

Disk Pulse 9.7.26 - 'Add Directory' Local Buffer Overflow
| windows/local/4[01;31m[K21[m[K63.py
```

```
Disk Sorter 9.7.14 - 'Input Directory' Local Buffer Overflow
| windows/local/4[01;31m[K21[m[K57.py

Disk Sorter 9.7.14 - 'Input Directory' Local Buffer Overflow (PoC)
| windows/dos/4[01;31m[K21[m[K12.py

DiskBoss 8.0.16 - 'Input Directory' Local Buffer Overflow
| windows/local/4[01;31m[K21[m[K60.py

dislocate 1.3 - Local i386
| linux/local/[01;31m[K21[m[K6.c

Dispair 0.1/0.2 - Remote Command Execution
| cgi/webapps/[01;31m[K21[m[K679.txt

Divine Content Server 5.0 - Error Page Cross-Site Scripting
| cgi/webapps/23[01;31m[K21[m[K7.txt

DNRD 1.x/2.x - DNS Request/Reply Denial of Service
| unix/dos/[01;31m[K21[m[K236.txt

DNSTools 2.0 - Authentication Bypass
| php/webapps/[01;31m[K21[m[K425.txt

DNSTracer 1.8.1 - Buffer Overflow (PoC)
| linux/dos/4[01;31m[K21[m[K15.txt

docpile:we 0.2.2 - 'INIT_PATH' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K46.txt

DocsGPT 0.12.0 - Remote Code Execution
| python/webapps/5[01;31m[K21[m[K45.py

DokuWiki 2006-03-09b - 'dwpage.php' Remote Code Execution
| php/webapps/23[01;31m[K21[m[K.php

Domain Group Network GooCMS 1.02 - 'index.php' Cross-Site Scripting
| php/webapps/32[01;31m[K21[m[K8.txt

doorGets CMS 5.2 - SQL Injection
| php/webapps/315[01;31m[K21[m[K.txt

dotProject 0.2.1 - User Cookie Authentication Bypass
| php/webapps/[01;31m[K21[m[K661.txt

dotProject 2.0 - '/includes/db_connect.php?baseDir' Remote File
Inclusion                                 |
php/webapps/27[01;31m[K21[m[K8.txt

dotProject 2.0 - '/includes/session.php?baseDir' Remote File Inclusion
| php/webapps/27[01;31m[K21[m[K9.txt
```

```
dotProject 2.0 - '/modules/projects/gantt.php?dPconfig[root_dir]'
Remote File Inclusion                    |
php/webapps/27[01;31m[K21[m[K7.txt

dotProject 2.0 - '/modules/projects/vw_files.php?dPconfig[root_dir]'
Remote File Inclusion                |
php/webapps/272[01;31m[K21[m[K.txt

dotProject 2.0.4 - 'baseDir' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K91.txt

dotProject 2.1.9 - SQL Injection
| php/webapps/470[01;31m[K21[m[K.txt

Download Accelerator Plus DAP 8.6 - 'AniGIF.ocx' Buffer Overflow (PoC)
| windows/dos/6[01;31m[K21[m[K6.html

Download-Engine 1.4.2 - 'spaw' Remote File Inclusion
| php/webapps/25[01;31m[K21[m[K.txt

Dream4 Koobi Pro 5.6 - 'showtopic' SQL Injection
| php/webapps/28[01;31m[K21[m[K9.txt

Drobo 5N2 4.1.1 - Remote Command Injection
| hardware/remote/48[01;31m[K21[m[K4.py

Drupal 4.0 - News Message HTML Injection
| php/webapps/[01;31m[K21[m[K863.txt

Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution
| php/webapps/18[01;31m[K21[m[K.php

Drupal 5.[01;31m[K21[m[K/6.16 - Denial of Service
| php/dos/10826.sh

Druva inSync Windows Client 6.6.3 - Local Privilege Escalation
(PowerShell)                             |
windows/local/49[01;31m[K21[m[K1.ps1

DUdownload 1.0/1.1 - 'detail.asp' Multiple SQL Injections
| asp/webapps/29[01;31m[K21[m[K9.txt

Dup Scout Enterprise 10.0.18 - 'Import Command' Local Buffer Overflow
| windows/local/429[01;31m[K21[m[K.py

Dup Scout Enterprise 10.0.18 - 'online_registration' Remote Buffer
Overflow                                 |
windows/remote/49[01;31m[K21[m[K0.py

Dup Scout Enterprise 10.0.18 - 'sid' Remote Buffer Overflow (SEH)
| windows/remote/49[01;31m[K21[m[K7.py
```

DvBBS 2.0 - 'boardrule.php' SQL Injection
| php/webapps/33[01;31m[K21[m[K4.txt

Dynamic photo Gallery 1.02 - 'albumID' SQL Injection
| php/webapps/5[01;31m[K21[m[K1.txt

DynPage 1.0 - 'ckfinder' Multiple Arbitrary File Upload Vulnerabilities
| php/webapps/373[01;31m[K21[m[K.txt

E-Guest 1.1 - Server Side Include Arbitrary Command Execution
| linux/remote/[01;31m[K21[m[K586.txt

E-Xoopport 3.1 Module MyAnnonces - 'lid' SQL Injection
| php/webapps/9[01;31m[K21[m[K7.txt

e107 0.7.[01;31m[K21[m[K full - Remote File Inclusion / Cross-Site Scripting |
php/webapps/12818.txt

e107 0.7.8 - 'mailout.php' (Authenticated) Access Escalation
| php/webapps/37[01;31m[K21[m[K.pl

e107 < 0.7.11 - Arbitrary Variable Overwriting
| php/webapps/6[01;31m[K21[m[K9.txt

EA Battlefield 2 / Battlefield [01;31m[K21[m[K42 - Multiple Arbitrary File Upload Vulnerabilities |
windows/remote/14267.txt

EA Battlefield 2 1.41 / Battlefield [01;31m[K21[m[K42 1.50 - Multiple Denial of Service Vulnerabilities |
windows/dos/34093.txt

EarthStation 5 - Search Service Remote File Deletion
| windows/remote/23[01;31m[K21[m[K1.cpp

Easy DVD Creater 2.5.11 - Local Buffer Overflow (SEH)
| windows/local/425[01;31m[K21[m[K.py

Easy File Sharing Web Server 7.2 - 'POST' Remote Buffer Overflow
| windows/remote/4[01;31m[K21[m[K65.py

Easy File Sharing Web Server 7.2 - 'POST' Remote Buffer Overflow (DEP Bypass) |
windows/remote/4[01;31m[K21[m[K86.py

Easy File Sharing Web Server 7.2 - Authentication Bypass
| windows/remote/4[01;31m[K21[m[K59.txt

Easy LAN Folder Share 3.2.0.100 - Buffer Overflow
| windows/dos/26[01;31m[K21[m[K4.py

```
Easy MOV Converter 1.4.24 - 'Enter User Name' Local Buffer Overflow
(SEH)                                    |
windows/local/4[01;31m[K21[m[K74.py

Easynet4u Forum Host - 'forum.php' SQL Injection
| php/webapps/67[01;31m[K21[m[K.txt

EasyNews 1.5 - NewsDatabase/Template Modification
| php/webapps/[01;31m[K21[m[K168.txt

Eaton Network Shutdown Module 3.[01;31m[K21[m[K - Remote PHP Code
Injection                                                |
php/webapps/30059.py

eazyPortal 1.0.0 - Multiple Vulnerabilities
| php/webapps/109[01;31m[K21[m[K.txt

eBay Clone Script 2010 - 'showcategory.php' SQL Injection
| php/webapps/34[01;31m[K21[m[K6.txt

ec[01;31m[K21[m[K clone 3.0 - 'id' SQL Injection
| php/webapps/12459.txt

Ecartis 1.0.0/0.129 a Listar - Multiple Local Buffer Overflow
Vulnerabilities (1)                          |
linux/local/[01;31m[K21[m[K341.c

Ecartis 1.0.0/0.129 a Listar - Multiple Local Buffer Overflow
Vulnerabilities (2)                          |
linux/local/[01;31m[K21[m[K342.c

Echo Mirage 3.1 - Buffer Overflow (PoC)
| windows/dos/46[01;31m[K21[m[K6.py

EclipseBB 0.5.0 Lite - 'phpbb_root_path' Remote File Inclusion
| php/webapps/3[01;31m[K21[m[K4.pl

eCom Cart 1.3 - SQL Injection
| php/webapps/4[01;31m[K21[m[K51.txt

Ecometry SGDynamo 5.32/6.1/7.0 - Cross-Site Scripting
| windows/remote/[01;31m[K21[m[K446.txt

ECSIMAGING PACS 6.[01;31m[K21[m[K.5 - Remote code execution
| php/webapps/49388.txt

ECSIMAGING PACS 6.[01;31m[K21[m[K.5 - SQL injection
| php/webapps/49392.txt

eFront 3.6.14 (build 18012) - Multiple Persistent Cross-Site Scripting
Vulnerabilities                        |
php/webapps/30[01;31m[K21[m[K3.txt
```

```
EFS Easy Chat Server - Universal Buffer Overflow (SEH) (Metasploit)
| windows/remote/11[01;31m[K21[m[K0.rb

EFS Easy Chat Server 3.1 - Password Disclosure
| windows/webapps/4[01;31m[K21[m[K53.py

EFS Easy Chat Server 3.1 - Password Reset
| windows/webapps/4[01;31m[K21[m[K54.py

EFS Easy Chat Server 3.1 - Remote Buffer Overflow (SEH)
| windows/remote/4[01;31m[K21[m[K55.py

EFTP 2.0.7 337 - Remote Buffer Overflow Code Execution / Denial of
Service                                 |
windows/remote/[01;31m[K21[m[K109.c

EFTP Server 2.0.7.337 - Directory Existence / File Existence
| windows/remote/[01;31m[K21[m[K110.pl

eGroupWare 1.8.001.201104[01;31m[K21[m[K - Multiple Vulnerabilities
| php/webapps/17322.txt

Ehud Gavron TrACESroute 6.1.1 - Terminator Function Format String
| unix/local/[01;31m[K21[m[K516.pl

eIQnetworks License Manager - Remote Buffer Overflow (Metasploit) (3)
| windows/remote/[01;31m[K21[m[K40.py

EJ3 BlackBook 1.0 - 'footer.php' Multiple Cross-Site Scripting
Vulnerabilities                          |
php/webapps/317[01;31m[K21[m[K.txt

Ektron CMS 8.5.0 - Multiple Vulnerabilities
| asp/webapps/[01;31m[K21[m[K085.txt

Elaine's Realtime CRM Automation 6.18.17 - Reflected XSS
| php/webapps/5[01;31m[K21[m[K06.NA

Electrasoft 32Bit FTP 9.49.1 - Client Long Server Banner Buffer
Overflow                                |
windows/dos/222[01;31m[K21[m[K.pl

Elite Bulletin Board 2.1.[01;31m[K21[m[K - Multiple SQL Injections
| php/webapps/23575.txt

Elite Gaming Ladders 3.5 - 'match' SQL Injection
| php/webapps/1[01;31m[K21[m[K58.py

ElkarBackup 1.3.3 - 'Policy[name]' and 'Policy[Description]' Stored
Cross-site Scripting                    |
php/webapps/491[01;31m[K21[m[K.txt
```

```
EMC Centera Universal Access 4.0_4735.p4 - 'Username' SQL Injection
| php/webapps/3[01;31m[K21[m[K13.txt

EMC Data Protection Advisor DPA Illuminator - EJBInvokerServlet Remote
Code Execution                        |
windows/remote/30[01;31m[K21[m[K1.txt

EMC HomeBase Server - Directory Traversal Remote Code Execution
(Metasploit)                                |
windows/remote/17[01;31m[K21[m[K9.rb

Employee Performance Evaluation System 1.0 - 'Task and Description'
Persistent Cross Site Scripting        |
php/webapps/49[01;31m[K21[m[K5.txt

EmuMail 5.0 - Web Root Full Path Disclosure
| cgi/webapps/[01;31m[K21[m[K877.txt

EmuMail 5.0 Email Form - Script Injection
| cgi/webapps/[01;31m[K21[m[K878.txt

Endpoint Protector 4.0.4.0 - Multiple Vulnerabilities
| multiple/webapps/[01;31m[K21[m[K822.txt

EnGenius EnShare IoT Gigabit Cloud Service 1.4.11 - Remote Code
Execution                                   |
hardware/webapps/4[01;31m[K21[m[K14.py

Enhanced Multimedia Router 3.0.4.27 - Cross-Site Request Forgery (Add
Admin)                                    |
asp/webapps/48[01;31m[K21[m[K7.txt

Enterasys SSR8000 SmartSwitch - Port Scan Denial of Service
| hardware/dos/[01;31m[K21[m[K791.txt

Enthrallweb eHomes - 'homeDetail.asp?AD_ID' SQL Injection
| asp/webapps/291[01;31m[K21[m[K.txt

Epic Games Unreal Tournament Server 436.0 - Denial of Service Amplifier
| multiple/dos/[01;31m[K21[m[K593.txt

Epiphany 3.28.2.1 - Denial of Service
| multiple/dos/448[01;31m[K21[m[K.txt

Ericsson Network Location MPS GMPC[01;31m[K21[m[K - Privilege
Escalation (Metasploit)                                    |
multiple/webapps/50469.rb

Ericsson Network Location MPS GMPC[01;31m[K21[m[K - Remote Code
Execution (RCE) (Metasploit)                               |
multiple/webapps/50468.rb
```

```
Ero Auktion 2.0 - 'news.php' SQL Injection
| php/webapps/115[01;31m[K21[m[K.txt

ES Job Search Engine 3.0 - SQL Injection
| php/webapps/[01;31m[K21[m[K084.txt

ESCPUtil 1.15.2 2 - Printer Name Local Buffer Overflow
| linux/local/2[01;31m[K21[m[K90.txt

EServ 2.9x - Password-Protected File Access
| windows/remote/[01;31m[K21[m[K[01;31m[K21[m[K1.txt

Espinas CMS - SQL Injection
| asp/webapps/1[01;31m[K21[m[K00.txt

Essentia Web Server 2.1 - 'URL' Remote Buffer Overflow
| windows/remote/[01;31m[K21[m[K298.c

eStara SoftPhone 3.0.1 - SIP SDP Message Handling Format String Denial
of Service                          |
multiple/dos/27[01;31m[K21[m[K0.txt

eStara SoftPhone 3.0.1 SIP Packet - Multiple Malformed Field Denial of
Service Vulnerabilities             |
multiple/dos/27[01;31m[K21[m[K1.txt

eSyndiCat 1.6 - 'admin_lng' Cookie Authentication Bypass
| php/webapps/3[01;31m[K21[m[K01.txt

EternalMart Mailing List Manager 1.32 - Remote File Inclusion
| php/webapps/23[01;31m[K21[m[K8.txt

Ethereal 0.10.10 - 'SIP' Protocol Dissector Remote Buffer Overflow
| linux/remote/10[01;31m[K21[m[K.c

Ettercap 0.6.3.1 - Large Packet Buffer Overflow
| linux/remote/[01;31m[K21[m[K289.c

EType EServ 1.9x - NNTP Remote Denial of Service
| windows/dos/2[01;31m[K21[m[K24.pl

EType EServ 2.9x - FTP Remote Denial of Service
| windows/dos/2[01;31m[K21[m[K[01;31m[K21[m[K.pl

EType EServ 2.9x - POP3 Remote Denial of Service
| windows/dos/2[01;31m[K21[m[K22.pl

EType EServ 2.9x - SMTP Remote Denial of Service
| windows/dos/2[01;31m[K21[m[K23.pl

Eudora WorldMail 2.0 - Search Cross-Site Scripting
| cgi/webapps/230[01;31m[K21[m[K.txt
```

```
EVA-Web 2.1.2 - 'rubrique.php3?date' Cross-Site Scripting
| php/webapps/279[01;31m[K21[m[K.txt

Everest 5.50.[01;31m[K21[m[K00 - 'Open File' Denial of Service (PoC)
| windows/dos/48259.py

Evolvable Shambala Server 4.5 - Web Server Denial of Service
| windows/dos/[01;31m[K21[m[K498.c

eWebeditor - Directory Traversal
| asp/webapps/11[01;31m[K21[m[K2.txt

Exclusive Addons for Elementor 2.6.9 - Stored Cross-Site Scripting
(XSS)                                    |
multiple/webapps/5[01;31m[K21[m[K26.py

eXeem 0.[01;31m[K21[m[K - Local Password Disclosure
| windows/local/834.c

eXeem 0.[01;31m[K21[m[K - Local Password Disclosure (ASM)
| windows/local/844.asm

Exim - 'GHOST' glibc gethostbyname Buffer Overflow (Metasploit)
| linux/remote/364[01;31m[K21[m[K.rb

expect (/usr/bin/expect) - Local Buffer Overflow
| linux/local/[01;31m[K21[m[K8.c

Extcalendar 2.0b2 - 'cal_search.php' SQL Injection
| php/webapps/173[01;31m[K21[m[K.txt

Eyeball MessengerSDK 'CoVideoWindow.ocx' 5.0.907 - ActiveX Control
Remote Buffer Overflow                   |
windows/remote/3[01;31m[K21[m[K24.txt

EZ Publish 3.9.0/3.9.5/3.10.1 - Command Execution (Admin Required)
| php/webapps/74[01;31m[K21[m[K.txt

EZContents - 'minicalendar.php' Remote File Inclusion
| php/webapps/3[01;31m[K21[m[K16.txt

eZip Wizard 3.0 - Local Stack Buffer Overflow (Metasploit)
| windows/local/17[01;31m[K21[m[K0.rb

EZNE.NET Ezboard 2000 - Remote Buffer Overflow
| cgi/remote/[01;31m[K21[m[K287.pl

Ezylog Photovoltaic Management Server - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K273.txt

FactoSystem Weblog 0.9/1.0/1.1 - Multiple SQL Injections
| asp/webapps/[01;31m[K21[m[K766.txt
```

```
Factux - Local File Inclusion
| php/webapps/125[01;31m[K21[m[K.txt

Fake Identd 0.9/1.x - Client Query Remote Buffer Overflow
| linux/remote/[01;31m[K21[m[K663.c

Fantastic News 2.1.1 - SQL Injection
| php/webapps/273[01;31m[K21[m[K.txt

Fantastic News 2.1.3 - 'script_path' Remote File Inclusion
| php/webapps/22[01;31m[K21[m[K.txt

Faq-O-Matic 2.6/2.7 - Cross-Site Scripting
| cgi/remote/[01;31m[K21[m[K263.txt

FAROL - SQL Injection
| php/webapps/38[01;31m[K21[m[K3.txt

FastStone Image Viewer 4.6 - ReadAVonIP Crash (PoC)
| windows/dos/[01;31m[K21[m[K788.pl

Fedora [01;31m[K21[m[K setroubleshootd 3.2.22 - Local Privilege
Escalation                                                |
linux/local/36564.txt

Feindura File Manager 1.0(rc) - Arbitrary File Upload
| php/webapps/15[01;31m[K21[m[K7.txt

Feng Office 3.11.1.2 - SQL Injection
| php/webapps/5[01;31m[K21[m[K54.NA

Fetchmail 5.x - IMAP Reply Signed Integer Index
| unix/remote/[01;31m[K21[m[K066.c

Fetchmail 5.x - POP3 Reply Signed Integer Index
| unix/remote/[01;31m[K21[m[K064.c

FHEM 6.0 - Local File Inclusion
| php/webapps/486[01;31m[K21[m[K.txt

Fhimage 1.2.1 - Remote Command Execution (mq = off)
| php/webapps/78[01;31m[K21[m[K.pl

FIBARO System Home Center 5.0[01;31m[K21[m[K - Remote File Include
| multiple/webapps/48240.txt

FileBound 6.2 - Local Privilege Escalation
| windows/local/[01;31m[K21[m[K892.txt

FileCloud [01;31m[K21[m[K.2 - Cross-Site Request Forgery (CSRF)
| php/webapps/50774.txt
```

```
FileRun 2019.05.[01;31m[K21[m[K -  Reflected Cross-Site Scripting
| multiple/webapps/48607.txt

Filerun 20[01;31m[K21[m[K.03.26 - Remote Code Execution (RCE)
(Authenticated)                                          |
php/webapps/50313.py

FileWrangler 5.30 - Remote Stack Buffer Overflow (Metasploit)
| windows/remote/167[01;31m[K21[m[K.rb

FileZilla FTP Server 0.9.20b/0.9.[01;31m[K21[m[K - 'STOR' Denial of
Service                                                  |
windows/dos/2901.php

FileZilla FTP Server 0.9.[01;31m[K21[m[K - 'LIST/NLST' Denial of
Service                                                  |
windows/dos/2914.php

FiSH-irssi - Multiple Remote Buffer Overflow Vulnerabilities
| windows/dos/297[01;31m[K21[m[K.pl

FL Studio 10 Producer Edition - Buffer Overflow (SEH) (PoC)
| windows/dos/[01;31m[K21[m[K826.pl

FlashBB 1.1.8 - 'phpbb_root_path' Remote File Inclusion
| php/webapps/19[01;31m[K21[m[K.pl

FlashGet 3.x - IEHelper Remote Execution (PoC)
| windows/dos/110[01;31m[K21[m[K.txt

Flat Assembler 1.7.[01;31m[K21[m[K - Local Buffer Overflow
| linux/local/42265.py

flatCore 1.5 - Cross Site Request Forgery (CSRF)
| php/webapps/5[01;31m[K21[m[K66.txt

flatCore 1.5.5 - Arbitrary File Upload
| php/webapps/5[01;31m[K21[m[K65.txt

FlatNuke 2.5.6 - 'ID' Directory Traversal
| php/webapps/26[01;31m[K21[m[K2.txt

FlatNuke 2.5.6 - 'USR' Cross-Site Scripting
| php/webapps/26[01;31m[K21[m[K5.txt

FlatNuke 2.5.7 - 'index.php' Remote File Inclusion
| php/webapps/28[01;31m[K21[m[K6.txt

flatnux 20[01;31m[K21[m[K-03.25 - Remote Code Execution (Authenticated)
| php/webapps/51295.txt

Flatpress 0.804 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/324[01;31m[K21[m[K.html
```

```
FlightPath < 4.8.2 / < 5.0-rc2 - Local File Inclusion
| php/webapps/471[01;31m[K21[m[K.txt

Flowerfire Sawmill 5.0.[01;31m[K21[m[K - File Access
| cgi/remote/20041.txt

Flowerfire Sawmill 5.0.[01;31m[K21[m[K - Weak Password Encryption
| unix/local/20042.c

Fluid Dynamics Search Engine 2.0 - Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K609.txt

FLV Players 8 - 'popup.php?url' Cross-Site Scripting
| multiple/remote/28[01;31m[K21[m[K0.txt

ForensiTAppxService 2.2.0.4 - 'ForensiTAppxService.exe' Unquoted
Service Path                                |
windows/local/488[01;31m[K21[m[K.txt

FormMail-Clone - Cross-Site Scripting
| cgi/webapps/2[01;31m[K21[m[K37.txt

Foro Domus 2.10 - 'phpbb_root_path' Remote File Inclusion
| php/webapps/3[01;31m[K21[m[K5.pl

Fortigate UTM WAF Appliance - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K21[m[K395.txt

Fortinet FortiClient 5.2.3 (Windows 10 x64 Pre-Anniversary) - Local
Privilege Escalation                    | windows_x86-
64/local/417[01;31m[K21[m[K.c

Forum 5 - 'pm.php' Local File Inclusion
| php/webapps/28[01;31m[K21[m[K7.txt

fowlcms 1.1 - Authentication Bypass / Local File Inclusion / Arbitrary
File Upload                           | php/webapps/85[01;31m[K21[m[K.txt

Foxit PDF Reader 4.1.1 - Title Stack Buffer Overflow (Metasploit)
| windows/local/166[01;31m[K21[m[K.rb

Foxit Reader 5.4.3.0920 - Crash (PoC)
| windows/dos/[01;31m[K21[m[K645.txt

Franklin Fueling Systems  TS-550 - Exploit and Default Password
| hardware/remote/513[01;31m[K21[m[K.txt

Free Hosting Manager 1.2/2.0 - Insecure Cookie Handling
| php/webapps/6[01;31m[K21[m[K3.txt

Free Image & File Hosting - Arbitrary File Upload
| php/webapps/1[01;31m[K21[m[K05.txt
```

FreeBSD 4.3/4.4 - Login Capabilities Privileged File Reading
| freebsd/local/[01;31m[K21[m[K114.txt

FreeBSD 4.4 - AIO Library Cross Process Memory Write
| freebsd/local/[01;31m[K21[m[K176.c

FreeBSD 4.x - Process Concealment Bypass
| freebsd/local/[01;31m[K21[m[K462.sh

FreeBSD 4.x / NetBSD 1.4.x/1.5.x/1.6 / OpenBSD 3 - pppd Arbitrary File Permission Modification Race Condit | bsd/local/[01;31m[K21[m[K669.pl

FreeBSD Kernel (FreeBSD 10.2 < 10.3 x64) - 'SETFKEY' (PoC)
| freebsd_x86-64/dos/44[01;31m[K21[m[K1.c

FreeBSD Kernel (FreeBSD 10.2 x64) - 'sendmsg' Kernel Heap Overflow (PoC) | freebsd_x86-64/dos/44[01;31m[K21[m[K2.c

freeForum 1.7 - 'acuparam' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K39.txt

FreePBX 2.11.0 - Remote Command Execution
| php/webapps/32[01;31m[K21[m[K4.pl

FreeQBoard 1.0/1.1 - 'QB_Path' Multiple Remote File Inclusions
| php/webapps/29[01;31m[K21[m[K5.txt

freeSSHd 1.2 - 'SSH2_MSG_NEWKEYS' Remote Denial of Service
| linux/dos/31[01;31m[K21[m[K8.txt

Freeway CMS 1.4.3.[01;31m[K21[m[K0 - SQL Injection
| php/webapps/14474.txt

FreeWebShop 2.2.9 R2 - 'ajax_save_name.php' Remote Code Execution
| php/webapps/181[01;31m[K21[m[K.txt

FreeWnn 1.1 0 - jserver JS_MKDIR MetaCharacter Command Execution
| unix/remote/[01;31m[K21[m[K[01;31m[K21[m[K5.c

Frox 0.7.18 - Arbitrary Configuration File Access
| linux/local/26[01;31m[K21[m[K8.txt

FS Makemytrip Clone - 'id' SQL Injection
| php/webapps/43[01;31m[K21[m[K3.txt

FS Shaadi Clone - 'token' SQL Injection
| php/webapps/43[01;31m[K21[m[K5.txt

FSphp 0.2.1 - Remote File Inclusion
| php/webapps/98[01;31m[K21[m[K.txt

```
FsPro Labs Event Log Explorer v4.6.1.[01;31m[K21[m[K15 - XML External
Entity Injection                                  |
windows/webapps/45319.txt

FTPGetter 3.58.0.[01;31m[K21[m[K - 'PASV' Remote Buffer Overflow
| windows/remote/16101.py

FTPshell Server 3.38 - Remote Denial of Service
| windows/dos/11[01;31m[K21[m[K.pl

ftpzik - Cross-Site Scripting / Local File Inclusion
| php/webapps/7[01;31m[K21[m[K4.txt

Fully Modded phpBB 20[01;31m[K21[m[K.4.40 - Multiple File Inclusions
| php/webapps/26[01;31m[K21[m[K.txt

FunkBoard 0.66 - 'profile.php' Multiple Cross-Site Scripting
Vulnerabilities                                   |
php/webapps/261[01;31m[K21[m[K.txt

FuseTalk 4.0 - 'AuthError.cfm' Multiple Cross-Site Scripting
Vulnerabilities                                   |
cfm/webapps/30[01;31m[K21[m[K6.txt

FusionForge 5.0 - Multiple Remote File Inclusions
| php/webapps/1[01;31m[K21[m[K79.txt

Gafware CFXImage 1.6.4/1.6.6 - ShowTemp File Disclosure
| cfm/webapps/[01;31m[K21[m[K493.txt

Galacticomm Worldgroup 3.20 - Remote FTP Denial of Service
| windows/dos/[01;31m[K21[m[K305.c

Galacticomm Worldgroup 3.20 - Remote Web Server Denial of Service
| windows/dos/[01;31m[K21[m[K306.c

Galaxy FTP Server 1.0 (Neostrada Livebox DSL Router) - Denial of
Service                                           |
linux/dos/5[01;31m[K21[m[K0.c

Gallarific 1.1 - '/gallery.php' Arbitrary Delete/Edit Category
| php/webapps/94[01;31m[K21[m[K.txt

Games Script - 'Galore' Backup Dump
| php/webapps/1[01;31m[K21[m[K98.txt

GameSpy 3D 2.62 - Packet Amplification Denial of Service
| linux/dos/2[01;31m[K21[m[K83.c

GarageSales - Arbitrary File Upload
| php/webapps/1[01;31m[K21[m[K28.txt
```

```
GattLib 0.2 - Stack Buffer Overflow
| linux/remote/46[01;31m[K21[m[K5.rb

Gaucho 1.4 - Mail Client Buffer Overflow
| windows/remote/4[01;31m[K21[m[K.c

gBook 1.4 - Administrative Access
| php/webapps/[01;31m[K21[m[K960.txt

GDAM123 0.933/0.942 - Filename Buffer Overflow
| unix/local/[01;31m[K21[m[K760.c

GE Fanuc Real Time Information Portal 2.6 - 'writeFile()' API
(Metasploit)                                |
windows/remote/69[01;31m[K21[m[K.rb

GeekHelps ADMP 1.01 - Multiple Vulnerabilities
| php/webapps/117[01;31m[K21[m[K.txt

Geeklog 1.3.5 - Calendar Event Form Script Injection
| php/webapps/[01;31m[K21[m[K528.txt

Geeklog 1.3.5 - HTML Attribute Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K628.txt

Geeklog 1.3.5 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K21[m[K525.txt

Geeklog 1.3.7 - 'comment.php?cid' Cross-Site Scripting
| php/webapps/2[01;31m[K21[m[K65.txt

Geeklog 1.3.7 - 'Homepage User' HTML Injection
| php/webapps/2[01;31m[K21[m[K66.txt

Geeklog 1.3.7 - 'profiles.php' Multiple Cross-Site Scripting
Vulnerabilities                             |
php/webapps/2[01;31m[K21[m[K63.txt

Geeklog 1.3.7 - 'users.php?uid' Cross-Site Scripting
| php/webapps/2[01;31m[K21[m[K64.txt

GeniXCMS 0.0.1 - Multiple Vulnerabilities
| php/webapps/363[01;31m[K21[m[K.txt

GeoBlog MOD_1.0 - 'deleteblog.php?id' Arbitrary Blog Deletion
| php/webapps/303[01;31m[K21[m[K.txt

GeoVision Geowebserver 5.3.3 - Local FIle Inclusion
| hardware/webapps/50[01;31m[K21[m[K1.txt

GeoVision GV-ASManager 6.1.0.0  - Information Disclosure
| multiple/webapps/5[01;31m[K21[m[K44.txt
```

GeoVision GV-ASManager 6.1.0.0 - Broken Access Control
| multiple/webapps/5[01;31m[K21[m[K89.txt

GeoVision GV-ASManager 6.1.1.0 - CSRF
| multiple/webapps/5[01;31m[K21[m[K87.txt

Gert Doering mgetty 1.1.19/1.1.20/1.1.[01;31m[K21[m[K/1.22.8 - Symbolic Link Traversal | unix/local/20179.txt

GetGo Download Manager 4.9.0.1982 - HTTP Response Header Buffer Overflow Remote Code Execution | windows/remote/3[01;31m[K21[m[K32.py

GetSimpleCMS 3.3.16 - Remote Code Execution (RCE)
| php/webapps/5[01;31m[K21[m[K68.txt

GGZ Gaming Zone 0.0.12 - Multiple Denial of Service Vulnerabilities
| multiple/dos/274[01;31m[K21[m[K.txt

GHIA CamIP 1.2 for iOS - 'Password' Denial of Service (PoC)
| ios/dos/477[01;31m[K21[m[K.py

Ghostscript 9.20 - 'Filename' Command Execution
| windows/local/412[01;31m[K21[m[K.txt

Ghostscript 9.[01;31m[K21[m[K - Type Confusion Arbitrary Command Execution (Metasploit) | linux/local/41955.rb

ghttpd 1.4.x - 'Log()' Remote Buffer Overflow
| linux/remote/[01;31m[K21[m[K937.c

GitLab Community Edition (CE) 13.10.3 - User Enumeration
| ruby/webapps/498[01;31m[K21[m[K.sh

GL.iNet AR300M v3.[01;31m[K21[m[K6 Remote Code Execution - CVE-2023-46456 Exploit | hardware/remote/51854.py

glFTPd 1.x - 'LIST' Denial of Service
| unix/dos/[01;31m[K21[m[K074.pl

glFusion 1.x - SQL Injection
| php/webapps/366[01;31m[K21[m[K.txt

glibc - NUL Byte gconv_translit_find Off-by-One
| linux/local/344[01;31m[K21[m[K.c

GLIBC locale - bug mount
| linux/local/[01;31m[K21[m[K5.c

GlobalScape CuteFTP 5.0 - LIST Response Buffer Overflow
| windows/remote/2[01;31m[K21[m[K84.pl

GlobalSunTech Access Point GL2422AP-0T - Information Disclosure
| hardware/remote/[01;31m[K21[m[K983.c

Gnat-TGP 1.2.20 - Remote File Inclusion
| php/webapps/116[01;31m[K21[m[K.txt

GNOME esound 0.2.19 - Unix Domain Socket Race Condition
| unix/local/20[01;31m[K21[m[K2.txt

Gnome-PTY-Helper UTMP - Hostname Spoofing
| linux/local/263[01;31m[K21[m[K.c

GnomeHack - Local Buffer Overflow
| linux/local/[01;31m[K21[m[K9.c

GNU binutils - 'disassemble_bytes' Heap Overflow
| linux/dos/4[01;31m[K21[m[K99.txt

GNU binutils - 'rx_decode_opcode' Buffer Overflow
| linux/dos/4[01;31m[K21[m[K98.txt

GNU findutils 4.0/4.1 - Locate Arbitrary Command Execution
| linux/local/[01;31m[K21[m[K043.c

GNU groff 1.1x - xploitation Via LPD
| linux/remote/[01;31m[K21[m[K037.c

GNU Mailman 2.0.x - Admin Login Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K480.txt

GNU Mailman 2.0.x - Admin Login Variant Cross-Site Scripting
| cgi/remote/[01;31m[K21[m[K642.txt

GNU Mailman 2.0.x - Subscribe Cross-Site Scripting
| cgi/remote/[01;31m[K21[m[K641.txt

GNU Mailman 2.1 - 'email' Cross-Site Scripting
| cgi/webapps/2[01;31m[K21[m[K98.txt

GNU Mailman 2.1 - Error Page Cross-Site Scripting
| cgi/webapps/2[01;31m[K21[m[K99.txt

GNU Screen 3.9.x Braille Module - Local Buffer Overflow
| unix/local/[01;31m[K21[m[K414.c

Gnuboard5 5.3.2.8 - SQL Injection
| php/webapps/5[01;31m[K21[m[K67.txt

GNUJSP 1.0 - File Disclosure
| multiple/remote/[01;31m[K21[m[K295.txt

Go SSH servers 0.0.2 - Denial of Service (PoC)
| linux/dos/481[01;31m[K21[m[K.py

```
GoAhead Web Server 2.1 - Arbitrary Command Execution
| windows/remote/[01;31m[K21[m[K707.txt

GoAhead Web Server 2.1.x - Error Page Cross-Site Scripting
| windows/remote/[01;31m[K21[m[K608.txt

GoAhead Web Server 2.1.x - URL Encoded Slash Directory Traversal
| windows/remote/[01;31m[K21[m[K607.txt

GoAhead Web Server 2.18 - 'addgroup.asp?group' Cross-Site Scripting
| windows/remote/36[01;31m[K21[m[K7.txt

GoAhead Web Server 2.18 - 'addlimit.asp?url' Cross-Site Scripting
| windows/remote/36[01;31m[K21[m[K8.txt

GoAhead Web Server 2.18 - 'adduser.asp' Multiple Cross-Site Scripting
Vulnerabilities                      |
windows/remote/36[01;31m[K21[m[K9.txt

GOM Player 2.1.[01;31m[K21[m[K - '.avi' Denial of Service
| windows/dos/11724.pl

GOM Player 2.1.[01;31m[K21[m[K.4846 - '.wav' Buffer Overflow
| windows/dos/11536.pl

Gom Player 2.1.44.5123 - 'UNICODE' Null Pointer Dereference
| windows/dos/[01;31m[K21[m[K830.py

Google Android - '/system/bin/sdcard' Stack Buffer Overflow (PoC)
| android/dos/399[01;31m[K21[m[K.txt

Google Android - 'cfp_ropp_new_key_reenc' / 'cfp_ropp_new_key' RKP
Memory Corruption                        |
android/dos/41[01;31m[K21[m[K1.txt

Google Android - RKP EL1 Code Loading Bypass
| android/local/41[01;31m[K21[m[K7.txt

Google Android - RKP Information Disclosure via s2-remapping Physical
Ranges                                   |
android/dos/41[01;31m[K21[m[K8.txt

Google Android - Signature Verification Security Bypass
| android/remote/388[01;31m[K21[m[K.py

Google Android - Unprotected MSRs in EL1 RKP Privilege Escalation
| android/dos/41[01;31m[K21[m[K2.txt

Google Chrome - 'HTMLKeygenElement::shadowSelect()' Type Confusion
| multiple/dos/41[01;31m[K21[m[K4.html

Google Chrome - V8 Private Property Arbitrary Code Execution
| android/remote/4[01;31m[K21[m[K75.html
```

```
Google Chrome 72.0.3626.1[01;31m[K21[m[K / 74.0.3725.0 -
'NewFixedDoubleArray' Integer Overflow                          |
multiple/remote/46748.txt

Google Chrome 74.0.3729.0 / 76.0.3789.0 - Heap Use-After-Free in
blink::PresentationAvailabilityState::Upd |
multiple/dos/47[01;31m[K21[m[K1.html

Google Earth 5.1.3535.3[01;31m[K21[m[K8 - 'quserex.dll' DLL Hijacking
| windows/local/14790.c

Google Toolbar 1.1.60 - Search Function Denial of Service
| windows/dos/[01;31m[K21[m[K712.txt

Goople CMS 1.7 - Arbitrary Code Execution
| php/webapps/7[01;31m[K21[m[K0.txt

GotoCode Online Bookstore - Multiple Vulnerabilities
| asp/webapps/179[01;31m[K21[m[K.txt

Grav CMS 1.4.2 Admin Plugin - Cross-Site Scripting
| php/webapps/4[01;31m[K21[m[K31.txt

Greatclone GC Auction Platinum - 'category.php' SQL Injection
| php/webapps/3[01;31m[K21[m[K18.txt

GreyMatter WebLog 1.[01;31m[K21[m[Kd - Remote Command Execution (1)
| php/webapps/1618.c

GreyMatter WebLog 1.[01;31m[K21[m[Kd - Remote Command Execution (2)
| php/webapps/1619.pl

Group Office Calendar - '/calendar/json.php' SQL Injection
| php/webapps/[01;31m[K21[m[K056.txt

Grsecurity Kernel Patch 1.9.4 (Linux Kernel) - Memory Protection
| linux/local/[01;31m[K21[m[K458.txt

GStreamer gst-plugins-bad Plugin - NULL Pointer Dereference
| linux/dos/4[01;31m[K21[m[K62.txt

GuppY 2.4 - Cross-Site Scripting
| php/webapps/23[01;31m[K21[m[K9.txt

GuppY 4.5.16 - Remote Command Execution
| php/webapps/32[01;31m[K21[m[K.php

GV 2.x/3.x - '.PDF'/'.PS' File Buffer Overflow (1)
| linux/local/[01;31m[K21[m[K871.c

GV 2.x/3.x - '.PDF'/'.PS' File Buffer Overflow (2)
| linux/local/[01;31m[K21[m[K872.c
```

H-Sphere WebShell 2.4 - Local Privilege Escalation
| linux/local/2[01;31m[K21[m[K28.c

H-Sphere WebShell 2.4 - Remote Command Execution
| linux/remote/2[01;31m[K21[m[K29.c

H0tturk Panel - 'gizli.php' Remote File Inclusion
| php/webapps/3[01;31m[K21[m[K34.txt

Hacks List phpBB Mod 1.[01;31m[K21[m[K - SQL Injection
| php/webapps/2851.txt

Half-Life 1.1 Client - Server Message Format String
| windows/remote/2[01;31m[K21[m[K42.c

Half-Life AdminMod 2.50 Plugin - Remote Format String
| linux/remote/2[01;31m[K21[m[K41.c

Half-Life ClanMod 1.80/1.81 Plugin - Remote Format String
| multiple/remote/2[01;31m[K21[m[K39.c

Half-Life Server 1.1/3.1 - New Player Flood Denial of Service
| multiple/dos/[01;31m[K21[m[K572.txt

Half-Life StatsMe 2.6.x Plugin - CMD_ARGV Buffer Overflow
| multiple/remote/2[01;31m[K21[m[K38.c

Half-Life StatsMe 2.6.x Plugin - MakeStats Format String
| multiple/remote/2[01;31m[K21[m[K40.c

Hanso Converter 1.1.0 - BufferOverflow Denial of Service
| windows/dos/161[01;31m[K21[m[K.py

Hanterm 3.3 - Local Buffer Overflow (1)
| linux/local/[01;31m[K21[m[K280.c

Hanterm 3.3 - Local Buffer Overflow (2)
| linux/local/[01;31m[K21[m[K281.c

Harris Stratex StarMAX [01;31m[K21[m[K00 WIMAX Subscriber Station - Running Configuration Cross-Site Request Forgery | hardware/webapps/14264.html

Hashicorp vagrant-vmware-fusion 5.0.3 - Local Privilege Escalation
| macos/local/43[01;31m[K21[m[K9.sh

Hassan Consulting Shopping Cart 1.23 - Arbitrary Command Execution
| cgi/remote/[01;31m[K21[m[K104.pl

HCView - WriteAV Crash (PoC)
| windows/dos/[01;31m[K21[m[K785.pl

```
Heathco Software h2desk - Multiple Information Disclosure
Vulnerabilities                                    |
php/webapps/313[01;31m[K21[m[K.txt

Hedgehog-CMS 1.[01;31m[K21[m[K - 'header.php' Local File Inclusion
| php/webapps/5904.txt

Hedgehog-CMS 1.[01;31m[K21[m[K - Local File Inclusion / Remote Command
Execution                                          | php/webapps/8028.pl

Hedgehog-CMS 1.[01;31m[K21[m[K - Remote Command Execution
| php/webapps/8015.pl

Help Center Live 2.0.6 - 'module=helpcenter&file=' Local File Inclusion
| php/webapps/124[01;31m[K21[m[K.txt

Hex Workshop 6.0 - '.hex' Local Code Execution
| windows/local/81[01;31m[K21[m[K.pl

Hikvision IP Camera versions 5.2.0 - 5.3.9 (Builds 1407[01;31m[K21[m[K
< 170109) - Access Control Bypass                  | xml/webapps/44328.py

Hikvision Web Server Build [01;31m[K21[m[K0702 - Command Injection
| hardware/webapps/50441.py

Hitweb 4.2.1 - 'REP_INC' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K49.txt

HolaCMS 1.2/1.4.x Voting Module - Remote File Corruption
| php/webapps/25[01;31m[K21[m[K7.html

Home Web Server 1.9.1 (build 164) - Remote Code Execution
| windows/remote/4[01;31m[K21[m[K28.txt

Homes 4 Sale - 'results.php' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K41.txt

Honeywell Tema Remote Installer - ActiveX Remote Code Execution
(Metasploit)                                       |
windows/remote/240[01;31m[K21[m[K.rb

Horde 1.2.x/2.1.3 and Imp 2.2.x/3.1.2 - File Disclosure
| linux/remote/[01;31m[K21[m[K019.txt

Horde Groupware 5.2.[01;31m[K21[m[K - Unauthorized File Download
| php/webapps/44059.md

Horde Groupware Webmail Edition 5.2.22 - PHAR Loading
| php/webapps/48[01;31m[K21[m[K0.py

Horde Groupware Webmail Edition 5.2.22 - Remote Code Execution
| php/webapps/48[01;31m[K21[m[K5.sh
```

```
Horde IMP 2.2.x - Session Hijacking
| linux/remote/[01;31m[K21[m[K151.txt

Hosting Controller 1.4 - Import Root Directory Command Execution
| asp/webapps/[01;31m[K21[m[K457.txt

Hosting Controller 1.x - 'Browse.asp' File Disclosure
| asp/webapps/[01;31m[K21[m[K464.txt

Hosting Controller 1.x - DSNManager Directory Traversal
| asp/webapps/[01;31m[K21[m[K455.txt

HotNews 0.7.2 - Remote File Inclusion
| php/webapps/1[01;31m[K21[m[K60.txt

HP AdvanceStack Switch - Authentication Bypass
| hardware/remote/[01;31m[K21[m[K285.txt

HP Application Lifecycle Management - 'XGO.ocx' ActiveX
'SetShapeNodeType()' Remote Code Execution (Metasp |
windows/remote/[01;31m[K21[m[K842.rb

HP CIFS/9000 Server A.01.05/A.01.06 - Local Buffer Overflow
| hp-ux/local/[01;31m[K21[m[K577.c

HP Compaq Insight Manager - Web Interface Cross-Site Scripting
| hardware/remote/[01;31m[K21[m[K827.txt

HP Data Protector - Backup Client Service Remote Code Execution
(Metasploit)                                |
windows/remote/3[01;31m[K21[m[K64.rb

HP Data Protector 6.1 - EXEC_CMD Remote Code Execution (Metasploit)
| windows/remote/185[01;31m[K21[m[K.rb

HP Data Protector Media Operations - Null Pointer Dereference Remote
Denial of Service                     |
windows_x86/dos/15[01;31m[K21[m[K4.py

HP LaserJet Professional M1[01;31m[K21[m[K0 MFP Series Receive Fax
Service - Unquoted Service Path                       |
windows/local/50959.txt

HP OfficeJet 4630/7110 MYM1FN2025AR/[01;31m[K21[m[K17A - Stored Cross-
Site Scripting (XSS)                                  |
hardware/webapps/50227.py

HP Operations Dashboard 2.1 - Portal Default Manager Account Remote
Security                                |
multiple/remote/33[01;31m[K21[m[K1.txt

HP Operations Manager - Default Manager 8.1 Account Remote Security
| multiple/remote/33[01;31m[K21[m[K0.txt
```

HP PageWide Printers / HP OfficeJet Pro Printers (OfficeJet Pro
8[01;31m[K21[m[K0) - Arbitrary Code Execution |
hardware/remote/4[01;31m[K21[m[K76.py

HP Procurve 4000M Switch - Device Reset Denial of Service
| hardware/dos/[01;31m[K21[m[K828.txt

HP ProCurve Switch 4000M - SNMP Write Denial of Service
| hardware/dos/[01;31m[K21[m[K657.txt

HP ProCurve Threat Management Services - zl ST.1.0.090[01;31m[K21[m[K3
Module CRL Security Bypass |
multiple/remote/33078.txt

HP SiteScope (Linux/Windows) - Remote Code Execution (Metasploit)
| multiple/remote/[01;31m[K21[m[K137.rb

HP Tru64 - NLSPATH Environment Variable Local Buffer Overflow (1)
| unix/local/[01;31m[K21[m[K772.pl

HP Tru64 - NLSPATH Environment Variable Local Buffer Overflow (2)
| unix/local/[01;31m[K21[m[K773.pl

HP Tru64 4.0/5.0/5.1 - _XKB_CHARSET Local Buffer Overflow
| unix/local/[01;31m[K21[m[K774.pl

HP Tru64/OSF1 DXTerm - Local Buffer Overflow
| unix/local/[01;31m[K21[m[K807.pl

HP-UX 11.0 - SWVerify Buffer Overflow
| hp-ux/local/[01;31m[K21[m[K098.c

HP-UX 7-11 - X Font Server Local Buffer Overflow
| hp-ux/local/24[01;31m[K21[m[K0.pl

HP-UX FTPD - Remote Buffer Overflow
| hp-ux/dos/[01;31m[K21[m[K2.c

HP-UX FTPD 1.1.[01;31m[K21[m[K4.4 - 'REST' Memory Disclosure
| hp-ux/remote/22733.c

HP-UX FTPD 1.1.[01;31m[K21[m[K4.4 - 'REST' Remote Brute Force
| hp-ux/remote/977.c

HTML5 Video Player 1.2.5 - Buffer Overflow (Metasploit)
| windows/local/459[01;31m[K21[m[K.rb

HttpBlitz Web Server - Denial of Service
| windows/dos/158[01;31m[K21[m[K.py

Huawei E5330 [01;31m[K21[m[K.[01;31m[K21[m[K0.09.00.158 - Cross-Site
Request Forgery (Send SMS) |
hardware/webapps/46092.py

Huawei E5331 MiFi Mobile Hotspot [01;31m[K21[m[K.344.11.00.414 - Multiple Vulnerabilities | hardware/webapps/3[01;31m[K21[m[K61.txt

Huawei HedEx Lite 200R006C00SPC005 - Path Traversal | windows/remote/49[01;31m[K21[m[K8.txt

Huawei Technologies Internet Mobile - Unicode (SEH) | windows/local/[01;31m[K21[m[K988.pl

Hyena Cart - 'index.php' SQL Injection | php/webapps/16[01;31m[K21[m[K3.txt

i.FTP 2.[01;31m[K21[m[K - Host Address / URL Field (SEH) | windows/dos/39782.py

i.FTP 2.[01;31m[K21[m[K - Overflow Crash (SEH) (PoC) | windows/dos/36847.py

i.FTP 2.[01;31m[K21[m[K - Time Field (SEH) | windows/remote/36984.py

Iatek PortalApp 3.3/4.0 - 'login.asp' Multiple Cross-Site Scripting Vulnerabilities | asp/webapps/342[01;31m[K21[m[K.txt

iBall Baton iB-WRA150N - DNS Change | hardware/webapps/4[01;31m[K21[m[K92.sh

iBill Management Script - Weak Hard-Coded Password | cgi/remote/[01;31m[K21[m[K129.java

IBM ACPRunner 1.2.5 - ActiveX Control Dangerous Method | windows/remote/24[01;31m[K21[m[K9.txt

IBM AIX 4.2.1 / Sun Solaris 7.0 - LC_MESSAGES libc Buffer Overflow (1) | aix/local/19[01;31m[K21[m[K3.sh

IBM AIX 4.2.1 / Sun Solaris 7.0 - LC_MESSAGES libc Buffer Overflow (2) | aix/local/19[01;31m[K21[m[K4.c

IBM AIX 4.2.1 / Sun Solaris 7.0 - LC_MESSAGES libc Buffer Overflow (3) | aix/local/19[01;31m[K21[m[K5.c

IBM AIX 4.2.1 / Sun Solaris 7.0 - LC_MESSAGES libc Buffer Overflow (4) | aix/local/19[01;31m[K21[m[K6.c

IBM AIX 4.2.1 / Sun Solaris 7.0 - LC_MESSAGES libc Buffer Overflow (5) | aix/local/19[01;31m[K21[m[K7.c

IBM AIX 4.3.x/5.1 - 'ERRPT' Local Buffer Overflow | aix/local/[01;31m[K21[m[K904.pl

IBM HTTP Server 1.3.x - Source Code Disclosure
| multiple/remote/[01;31m[K21[m[K145.nasl

IBM Informix Dynamic Server - Code Injection / Remote Code Execution
| linux/webapps/4[01;31m[K21[m[K87.py

IBM Informix SE 7.25 sqlexec - Local Buffer Overflow (1)
| linux/local/[01;31m[K21[m[K496.c

IBM Informix SE 7.25 sqlexec - Local Buffer Overflow (2)
| linux/local/[01;31m[K21[m[K497.pl

ibm informix Web Datablade 3.x/4.1 - Directory Traversal
| multiple/remote/[01;31m[K21[m[K160.txt

IBM Informix Web Datablade 4.1x - Page Request SQL Injection
| cgi/webapps/[01;31m[K21[m[K374.txt

IBM Security Verify Access 10.0.0 - Open Redirect during OAuth Flow
| multiple/webapps/5[01;31m[K21[m[K23.NA

IBM System Storage DS Storage Manager Profiler - Multiple
Vulnerabilities |
windows/webapps/193[01;31m[K21[m[K.txt

IBM Tivoli Identity Manager 5.0.5 - User Profile HTML Injection
| multiple/remote/33[01;31m[K21[m[K5.txt

IBM Tivoli Storage Manager Express CAD Service - Remote Buffer Overflow
(Metasploit) (1) |
windows/remote/164[01;31m[K21[m[K.rb

IBM Websphere Caching Proxy 3.6/4.0 - Denial of Service
| unix/dos/[01;31m[K21[m[K949.txt

IBM Websphere Edge Server 3.6/4.0 - Cross-Site Scripting
| unix/remote/[01;31m[K21[m[K947.txt

IBM Websphere Edge Server 3.69/4.0 - HTTP Header Injection
| unix/remote/[01;31m[K21[m[K948.txt

IBMi Navigator 7.5 - HTTP Security Token Bypass
| multiple/webapps/52[01;31m[K21[m[K0.txt

IBMi Navigator 7.5 - Server Side Request Forgery (SSRF)
| multiple/webapps/52[01;31m[K21[m[K2.txt

iCal 3.7 - HTTP Request Denial of Service
| windows/dos/2[01;31m[K21[m[K17.txt

iCal 3.7 - Remote Buffer Overflow (PoC)
| windows/dos/2[01;31m[K21[m[K18.txt

```
iCAM Workstation Control 4.8.0.0 - Authentication Bypass
| windows/local/3[01;31m[K21[m[K58.txt

Icecast 1.x - AVLLib Buffer Overflow
| unix/remote/[01;31m[K21[m[K363.c

icecast server 1.3.12 - Directory Traversal Information Disclosure
| linux/remote/[01;31m[K21[m[K602.txt

Iconics GENESIS32 9.[01;31m[K21[m[K.201.01 - Integer Overflow
(Metasploit)                                                |
windows/remote/17543.rb

ICQ For Mac OSX 2.6 Client - Denial of Service
| osx/dos/[01;31m[K21[m[K275.c

ICQ Toolbar 2.3 - ActiveX Remote Denial of Service
| windows/dos/5[01;31m[K21[m[K7.html

IcrediBB 1.1 - Script Injection
| php/webapps/[01;31m[K21[m[K399.txt

ID Software Quake 1.9 - Denial of Service
| multiple/dos/[01;31m[K21[m[K012.c

ID Software Quake 3 - 'SMURF' Denial of Service
| windows/dos/[01;31m[K21[m[K016.c

id Software Quake 3 Arena Server 1.29 - Buffer Overflow
| multiple/dos/[01;31m[K21[m[K042.txt

id Software Quake II Server 3.20/3.[01;31m[K21[m[K - Remote Information
Disclosure                                          |
multiple/remote/[01;31m[K21[m[K450.txt

iFTP 2.[01;31m[K21[m[K - Buffer Overflow Crash (PoC)
| windows/dos/37014.py

IKEView.exe R60 - '.elg' Local (SEH)
| windows/local/38[01;31m[K21[m[K8.py

IkonBoard 2.17/3.0/3.1 - Image Tag Cross-Agent Scripting
| php/webapps/[01;31m[K21[m[K304.txt

Ilia Alshanetsky FUDForum 1.2.8/1.9.8/2.0.2 - File Disclosure
| php/webapps/[01;31m[K21[m[K723.txt

Ilia Alshanetsky FUDForum 1.2.8/1.9.8/2.0.2 - File Modification
| php/webapps/[01;31m[K21[m[K724.txt

Image Display System 0.8.1 - Directory Existence Disclosure
| cgi/webapps/[01;31m[K21[m[K487.pl
```

```
Image22 ActiveX 1.1.1 - Remote Buffer Overflow
| windows/remote/143[01;31m[K21[m[K.html

Imatix Xitami 2.5 - GSL Template Cross-Site Scripting
| windows/remote/[01;31m[K21[m[K554.txt

iMesh 10.0 - 'IMWebControl.dll' ActiveX Control Buffer Overflow
| windows/remote/359[01;31m[K21[m[K.html

ImgSvr 0.6.[01;31m[K21[m[K - Error Message Remote Script Execution
| windows/remote/30939.txt

IMHO Webmail 0.9x - Account Hijacking
| cgi/webapps/[01;31m[K21[m[K617.txt

IMLib2 - Home Environment Variable Buffer Overflow
| linux/local/[01;31m[K21[m[K226.c

Indiatimes Messenger 6.0 - Remote Buffer Overflow
| windows/dos/26[01;31m[K21[m[K6.txt

InduSoft Web Studio - Arbitrary File Upload / Remote Code Execution
(Metasploit)                              |
windows/remote/[01;31m[K21[m[K837.rb

InfluxDB OSS 2.7.11 - Operator Token Privilege Escalation
| multiple/remote/5[01;31m[K21[m[K42.py

InfraPower PPS-02-S Q[01;31m[K21[m[K3V1 - Authentication Bypass
| php/webapps/40645.txt

InfraPower PPS-02-S Q[01;31m[K21[m[K3V1 - Cross-Site Request Forgery
| php/webapps/40646.txt

InfraPower PPS-02-S Q[01;31m[K21[m[K3V1 - Hard-Coded Credentials
| hardware/remote/40643.txt

InfraPower PPS-02-S Q[01;31m[K21[m[K3V1 - Insecure Direct Object
Reference                                                 |
php/webapps/40644.txt

InfraPower PPS-02-S Q[01;31m[K21[m[K3V1 - Local File Disclosure
| php/webapps/40642.txt

InfraPower PPS-02-S Q[01;31m[K21[m[K3V1 - Multiple Cross-Site Scripting
Vulnerabilities                                  | php/webapps/40641.txt

InfraPower PPS-02-S Q[01;31m[K21[m[K3V1 - Remote Command Execution
| hardware/webapps/40640.txt

Ingenium Learning Management System 5.1/6.1 - Reversible Password Hash
| multiple/remote/[01;31m[K21[m[K942.java
```

Inktomi Traffic Server 4/5 - Traffic_Manager Path Argument Buffer Overflow | linux/dos/[01;31m[K21[m[K580.txt

Inso DynaWeb HTTPd 3.1/4.0.2/4.1 - Format String | solaris/remote/[01;31m[K21[m[K678.c

Installshield 2009 15.0.0.53 Premier - 'ISWiAutomation15.dll' ActiveX Arbitrary File Overwrite | windows/remote/348[01;31m[K21[m[K.txt

Intego FileGuard 2.0/4.0 - Weak Password Encryption | osx/local/[01;31m[K21[m[K076.txt

Intelight X-1L Traffic controller Maxtime 1.9.6 - Remote Code Execution (RCE) | multiple/webapps/5[01;31m[K21[m[K51.txt

Intellinet IP Camera MNC-L10 - Authentication Bypass | hardware/webapps/145[01;31m[K21[m[K.txt

IntelliTamper 2.0.7 - HTML Parser Remote Buffer Overflow | windows/remote/61[01;31m[K21[m[K.c

IntelliTamper 2.07/2.08 - Defer Remote Buffer Overflow (PoC) | windows/dos/11[01;31m[K21[m[K7.txt

Interact 2.2 - 'CONFIG[base_path]' Remote File Inclusion | php/webapps/2[01;31m[K21[m[K8.txt

Interactive story 1.3 - Directory Traversal | cgi/remote/[01;31m[K21[m[K008.txt

Interbase 5/6 - GDS_Lock_MGR UMask File Permission Changing | linux/local/[01;31m[K21[m[K865.c

Interbase 6.0 - GDS_Drop Interbase Environment Variable Buffer Overflow (1) | unix/local/[01;31m[K21[m[K565.pl

Interbase 6.0 - GDS_Drop Interbase Environment Variable Buffer Overflow (2) | unix/local/[01;31m[K21[m[K566.c

Internet Download Manager - Local Buffer Overflow (SEH) | windows/local/[01;31m[K21[m[K320.pl

Internet Download Manager - Local Stack Buffer Overflow | windows/local/[01;31m[K21[m[K318.pl

Invoice System 1.0 - 'Multiple' Stored Cross-Site Scripting (XSS) | php/webapps/501[01;31m[K21[m[K.txt

ION Script 1.4 - Remote File Disclosure | cgi/webapps/[01;31m[K21[m[K979.txt

```
IPFire 2.19 - Remote Code Execution
| linux/webapps/4[01;31m[K21[m[K49.py

IPFire 2.[01;31m[K21[m[K - Cross-Site Scripting
| cgi/webapps/46344.txt

iPlanet Web Server 4.1 - Search Component File Disclosure
| multiple/remote/[01;31m[K21[m[K603.txt

IPSwitch IMail 6.x/7.0.x - Web Calendaring Incomplete Post Denial of
Service                                  |
windows/dos/[01;31m[K21[m[K673.txt

IPSwitch IMail 6.x/7.0/7.1 - Web Messaging GET Buffer Overflow
| windows/remote/[01;31m[K21[m[K654.c

Ipswitch WS_FTP Server 1.0.x/2.0.x - 'STAT' Remote Buffer Overflow
| windows/remote/[01;31m[K21[m[K142.pl

Ipswitch WS_FTP Server 2.0 - Anonymous Multiple FTP Command Buffer
Overflows                                  |
windows/remote/[01;31m[K21[m[K036.pl

IPTBB 0.5.4 - 'id' SQL Injection
| php/webapps/48[01;31m[K21[m[K.txt

IPUX CL5452/CL5132 IP Camera - 'UltraSVCamX.ocx' ActiveX Stack Buffer
Overflow                                 |
hardware/remote/354[01;31m[K21[m[K.txt

IrfanView 4.44 Email Plugin - Buffer Overflow (SEH)
| windows/local/44[01;31m[K21[m[K7.py

IrfanView 4.50 Email Plugin - Buffer Overflow (SEH Unicode)
| windows/local/44[01;31m[K21[m[K8.py

IRIX 6.5.x - Performance Co-Pilot Remote Denial of Service
| irix/dos/[01;31m[K21[m[K431.txt

IRSR 0.2 - '_sysSessionPath' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K99.txt

ISC BIND 9 - TKEY (PoC)
| multiple/dos/377[01;31m[K21[m[K.c

ISC DHCPD 2.0/3.0.1 - NSUPDATE Remote Format String
| bsd/remote/[01;31m[K21[m[K440.c

ISC INN 2.0/2.1/2.2.x - Multiple Local Format String Vulnerabilities
| linux/local/[01;31m[K21[m[K375.txt

ISDN4Linux 3.1 - IPPPD Device String SysLog Format String (1)
| linux/local/[01;31m[K21[m[K700.c
```

ISDN4Linux 3.1 - IPPPD Device String SysLog Format String (2)
| linux/local/[01;31m[K21[m[K701.pl

Iskratel SI2000 Callisto 8[01;31m[K21[m[K+ - Cross-Site Request Forgery
/ HTML Injection |
hardware/remote/35970.txt

IslamSound - Multiple SQL Injections
| php/webapps/339[01;31m[K21[m[K.txt

Isode M-Vault Server 11.3 - LDAP Memory Corruption
| multiple/dos/27[01;31m[K21[m[K2.txt

ISPworker 1.[01;31m[K21[m[K - 'download.php' Remote File Disclosure
| php/webapps/4592.txt

Istgah for Centerhost - Multiple Vulnerabilities
| php/webapps/1[01;31m[K21[m[K06.txt

iTech Gigs Script 1.[01;31m[K21[m[K - SQL Injection
| php/webapps/43096.txt

Ivanti Connect Secure 22.7R2.5 - Remote Code Execution (RCE)
| multiple/remote/52[01;31m[K21[m[K3.py

Jack De Winter WinSMTP 1.6 f/2.0 - Buffer Overflow
| windows/dos/202[01;31m[K21[m[K.pl

Jakarta Tomcat 3.x/4.0 - Error Message Information Disclosure
| unix/local/[01;31m[K21[m[K073.txt

JAMF Casper Suite MDM - Cross-Site Request Forgery
| jsp/webapps/[01;31m[K21[m[K545.txt

Jamroom 3.3.8 - Cookie Authentication Bypass
| php/webapps/3[01;31m[K21[m[K[01;31m[K21[m[K.php

Jaow 2.4.5 - Blind SQL Injection
| php/webapps/189[01;31m[K21[m[K.txt

Jasmin Ransomware - Arbitrary File Download (Authenticated)
| multiple/webapps/5[01;31m[K21[m[K40.txt

Jason Orcutt Prometheus 3.0/4.0/6.0 - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K976.txt

Java Deployment Toolkit - Performs Insufficient Validation of
Parameters |
windows/remote/1[01;31m[K21[m[K17.txt

JAVA Web Start - Arbitrary Command-Line Injection
| multiple/remote/1[01;31m[K21[m[K22.txt

Jaws 0.8.14 - Multiple Remote File Inclusions
| php/webapps/36[01;31m[K21[m[K6.txt

JBlog 1.0 - Create / Delete Admin Authentication Bypass
| php/webapps/4[01;31m[K21[m[K1.html

JBoss - DeploymentFileRepository WAR Deployment (via JMXInvokerServlet)
(Metasploit) |
multiple/remote/[01;31m[K21[m[K080.rb

JBoss 3.0.8/3.2.1 - HSQLDB Remote Command Injection
| multiple/remote/232[01;31m[K21[m[K.txt

Jetty 3.1.6/3.1.7/4.1 Servlet Engine - Arbitrary Command Execution
| cgi/webapps/[01;31m[K21[m[K895.txt

Jetty 4.1 Servlet Engine - Cross-Site Scripting
| jsp/webapps/[01;31m[K21[m[K875.txt

Jetty 9.4.37.v20[01;31m[K21[m[K0[01;31m[K21[m[K9 - Information
Disclosure |
java/webapps/50438.txt

jira 4.4.3 / greenhopper < 5.9.8 - Multiple Vulnerabilities
| jsp/webapps/[01;31m[K21[m[K052.txt

joelz bulletin board 0.9.9rc3 - Multiple SQL Injections
| php/webapps/1[01;31m[K21[m[K95.rb

John O'Fallon Responder.cgi 1.0 - Denial of Service
| cgi/dos/[01;31m[K21[m[K048.txt

John Roy Pi3Web 2.0 For Windows - Remote Buffer Overflow
| windows/remote/[01;31m[K21[m[K225.c

Jon Howell Faq-O-Matic 2.7 - Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K405.txt

Joomla! / Mambo Component com_lexikon - 'id' SQL Injection
| php/webapps/31[01;31m[K21[m[K4.txt

Joomla! / Mambo Component com_salesrep - 'rid' SQL Injection
| php/webapps/31[01;31m[K21[m[K3.txt

Joomla! / Mambo Component com_scheduling - 'id' SQL Injection
| php/webapps/31[01;31m[K21[m[K6.txt

Joomla! / Mambo Component com_sermon 0.2 - 'gid' SQL Injection
| php/webapps/311[01;31m[K21[m[K.txt

Joomla! / Mambo Component com_utchat 0.2 - Multiple Remote File
Inclusions |
php/webapps/3[01;31m[K21[m[K87.txt

Joomla! / Mambo Component Filebase - 'filecatid' SQL Injection
| php/webapps/31[01;31m[K21[m[K5.txt

Joomla! 1.5 Beta 2 - 'Search' Remote Code Execution
| php/webapps/4[01;31m[K21[m[K2.txt

Joomla! Component acctexp 0.12.x - Blind SQL Injection
| php/webapps/57[01;31m[K21[m[K.pl

Joomla! Component Address Book - Blind SQL Injection
| php/webapps/14[01;31m[K21[m[K0.txt

Joomla! Component Address Book 1.5.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K70.txt

Joomla! Component Advertising 0.25 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K71.txt

Joomla! Component Agenda Address Book 1.0.1 - 'id' SQL Injection
| php/webapps/1[01;31m[K21[m[K32.pl

Joomla! Component allvideos - Blind SQL Injection
| php/webapps/1[01;31m[K21[m[K37.txt

Joomla! Component AlphaUserPoints 1.5.5 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K50.txt

Joomla! Component Arcade Games 1.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K68.txt

Joomla! Component AWDwall 1.5.4 - Local File Inclusion / SQL Injection
| php/webapps/1[01;31m[K21[m[K13.txt

Joomla! Component aWiki - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K01.txt

Joomla! Component Candle 1.0 - 'cid' SQL Injection
| php/webapps/52[01;31m[K21[m[K.txt

Joomla! Component com_articles - SQL Injection
| php/webapps/1[01;31m[K21[m[K08.txt

Joomla! Component com_billyportfolio 1.1.2 - Blind SQL Injection
| php/webapps/157[01;31m[K21[m[K.txt

Joomla! Component com_book - SQL Injection
| php/webapps/11[01;31m[K21[m[K3.txt

Joomla! Component com_br - 'state_id' SQL Injection
| php/webapps/362[01;31m[K21[m[K.txt

Joomla! Component com_ca - SQL Injection
| php/webapps/1[01;31m[K21[m[K38.txt

Joomla! Component com_commedia - 'task' SQL Injection
| php/webapps/2[01;31m[K21[m[K52.txt

Joomla! Component com_expedition - 'id' SQL Injection
| php/webapps/36[01;31m[K21[m[K5.txt

Joomla! Component com_horses - 'id' SQL Injection
| php/webapps/340[01;31m[K21[m[K.txt

Joomla! Component com_jajobboard - Multiple Local File Inclusions
| php/webapps/1[01;31m[K21[m[K44.txt

Joomla! Component com_jdrugstopics - SQL Injection
| php/webapps/1[01;31m[K21[m[K83.txt

Joomla! Component com_kunena - 'search' SQL Injection
| php/webapps/2[01;31m[K21[m[K53.pl

Joomla! Component com_mediaalert - 'id' SQL Injection
| php/webapps/33[01;31m[K21[m[K8.txt

Joomla! Component com_pcchess - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K23.txt

Joomla! Component com_pressrelease - 'id' SQL Injection
| php/webapps/33[01;31m[K21[m[K7.txt

Joomla! Component com_qcontacts 1.0.6 - SQL Injection
| php/webapps/18[01;31m[K21[m[K8.txt

Joomla! Component com_record - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K81.txt

Joomla! Component com_sef - Local File Inclusion
| php/webapps/14[01;31m[K21[m[K3.txt

Joomla! Component com_spsnewsletter - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K49.txt

Joomla! Component com_surveymanager 1.5.0 - 'stype' SQL Injection
| multiple/webapps/97[01;31m[K21[m[K.txt

Joomla! Component com_ticketbook - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K43.txt

Joomla! Component com_webeecomment 2.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K11.txt

Joomla! Component com_worldrates - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K80.txt

Joomla! Component CV Maker 1.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K72.txt

Joomla! Component Digital Diary 1.5.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K78.txt

Joomla! Component Easy Shop 1.2.3 - Local File Inclusion
| php/webapps/46[01;31m[K21[m[K9.txt

Joomla! Component Easydiscuss < 4.0.[01;31m[K21[m[K - Cross-Site Scripting |
php/webapps/43488.txt

Joomla! Component education - SQL Injection
| php/webapps/1[01;31m[K21[m[K53.txt

Joomla! Component Flash Uploader 2.5.1 - Remote File Inclusion
| php/webapps/45[01;31m[K21[m[K.txt

Joomla! Component FlashGames 1.5.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K69.txt

Joomla! Component FLEXIcontent 1.5 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K85.txt

Joomla! Component Foobla Suggestions 1.5.1.2 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K20.txt

Joomla! Component Horoscope 1.5.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K67.txt

Joomla! Component Huru Helpdesk - SQL Injection (1)
| php/webapps/1[01;31m[K21[m[K24.txt

Joomla! Component JA Voice 2.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K[01;31m[K21[m[K.txt

Joomla! Component JD-Wiki 1.0.2 - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K25.txt

Joomla! Component Jfeedback 1.2 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K45.txt

Joomla! Component JoomMail 1.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K75.txt

Joomla! Component JoomProject 1.1.3.2 - Information Disclosure
| php/webapps/461[01;31m[K21[m[K.txt

Joomla! Component JoomRecipe 1.0.3 - SQL Injection
| php/webapps/4[01;31m[K21[m[K85.txt

Joomla! Component JP Jobs 1.2.0 - 'id' SQL Injection
| php/webapps/1[01;31m[K21[m[K91.txt

Joomla! Component JProject Manager 1.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K46.txt

Joomla! Component JS Support Ticket (component com_jssupportticket)
1.1.5 - Arbitrary File Download |
php/webapps/47[01;31m[K21[m[K6.txt

Joomla! Component JS Support Ticket (component com_jssupportticket)
1.1.5 - SQL Injection |
php/webapps/47[01;31m[K21[m[K8.txt

Joomla! Component JTicketing 2.0.16 - SQL Injection
| php/webapps/441[01;31m[K21[m[K.txt

Joomla! Component Jvehicles 1.0/2.0 - 'aid' SQL Injection
| php/webapps/1[01;31m[K21[m[K90.txt

Joomla! Component JVideo 0.3.x - SQL Injection
| php/webapps/88[01;31m[K21[m[K.txt

Joomla! Component Kochsuite 0.9.4 - Remote File Inclusion
| php/webapps/2[01;31m[K21[m[K5.txt

Joomla! Component Link Directory 1.0.3 - Remote File Inclusion
| php/webapps/2[01;31m[K21[m[K4.txt

Joomla! Component Memory Book 1.2 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K76.txt

Joomla! Component Multi-Venue Restaurant Menu Manager 1.5.2 - SQL
Injection |
php/webapps/1[01;31m[K21[m[K59.txt

Joomla! Component mv_restaurantmenumanager - SQL Injection
| php/webapps/1[01;31m[K21[m[K62.txt

Joomla! Component My Files 1.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K73.txt

Joomla! Component mygallery - 'farbinform_krell' SQL Injection
| php/webapps/10[01;31m[K21[m[K4.txt

Joomla! Component NinjaMonials - Blind SQL Injection
| php/webapps/14[01;31m[K21[m[K1.txt

Joomla! Component Online Exam 1.5.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K74.txt

Joomla! Component Online Market 2.x - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K77.txt

Joomla! Component Payage 2.05 - 'aid' SQL Injection
| php/webapps/4[01;31m[K21[m[K13.txt

Joomla! Component Poll 1.0.10 - Arbitrary Add Votes
| php/webapps/2[01;31m[K21[m[K9.php

Joomla! Component PowerMail Pro 1.5.3 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K18.txt

Joomla! Component Preventive And Reservation 1.0.5 - Local File Inclusion |
php/webapps/1[01;31m[K21[m[K47.txt

Joomla! Component Real Estate Property 3.1.22-03 - 'aid' SQL Injection
| php/webapps/1[01;31m[K21[m[K36.txt

Joomla! Component Realtyna Translator 1.0.15 - Local File Inclusion (1)
| php/webapps/1[01;31m[K21[m[K12.txt

Joomla! Component RokModule 1.1 - 'module' Blind SQL Injection
| php/webapps/[01;31m[K21[m[K2[01;31m[K21[m[K.txt

Joomla! Component RokModule 1.1 - 'moduleid' Blind SQL Injection
| php/webapps/1[01;31m[K21[m[K48.txt

Joomla! Component SermonSpeaker - SQL Injection
| php/webapps/1[01;31m[K21[m[K84.txt

Joomla! Component Sweetykeeper 1.5 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K82.txt

Joomla! Component TRAVELbook 1.0.1 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K51.txt

Joomla! Component TweetLA 1.0.1 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K42.txt

Joomla! Component VJDEO 1.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K02.txt

Joomla! Component Web TV 1.0 - Local File Inclusion
| php/webapps/1[01;31m[K21[m[K66.txt

Joomla! Component Webring 1.0 - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K77.txt

JPEGsnoop 1.5.2 - WriteAV Crash (PoC)
| windows/dos/[01;31m[K21[m[K739.pl

jQuery 3.3.1 - Prototype Pollution & XSS Exploit
| multiple/webapps/5[01;31m[K21[m[K41.txt

jQuery Uploadify 2.1.0 - Arbitrary File Upload
| multiple/webapps/11[01;31m[K21[m[K8.txt

Jurpopage 0.2.0 - SQL Injection
| php/webapps/156[01;31m[K21[m[K.txt

JVC IP-Camera VN-T[01;31m[K21[m[K6VPRU - Credentials Disclosure
| cgi/webapps/40264.txt

JVC IP-Camera VN-T[01;31m[K21[m[K6VPRU - Local File Disclosure
| cgi/webapps/40282.txt

K7 Ultimate Security K7RKScan.sys 17.0.2019 - Denial Of Service (DoS)
| multiple/remote/5[01;31m[K21[m[K58.py

KAPhotoservice - 'order.asp?page' Cross-Site Scripting
| asp/webapps/3[01;31m[K21[m[K84.txt

KAPhotoservice - 'search.asp?Filename' Cross-Site Scripting
| asp/webapps/3[01;31m[K21[m[K85.txt

Karel IP Phone IP1[01;31m[K21[m[K1 Web Management Panel - Directory Traversal |
hardware/webapps/48857.txt

Kaseya Virtual System Administrator (VSA) - Multiple Vulnerabilities (1) |
windows/webapps/376[01;31m[K21[m[K.txt

Kaspersky KSN for Linux 5.2 - Memory Corruption
| linux/dos/445[01;31m[K21[m[K.py

Kayako eSupport 2.3.1 - 'subd' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K15.txt

Kayako SupportSuite 3.x - '/staff/index.php?customfieldlinkid' SQL Injection |
php/webapps/322[01;31m[K21[m[K.txt

Kayako SupportSuite 3.x - '/visitor/index.php?sessionid' Cross-Site Scripting |
php/webapps/32[01;31m[K21[m[K9.txt

KaZaA Media Desktop 1.7.1 - Large Message Denial of Service
| windows/dos/[01;31m[K21[m[K653.c

KBVault MySQL 0.16a - Arbitrary File Upload
| aspx/webapps/4[01;31m[K21[m[K84.txt

KDE 3.0.x - KPF Icon Option File Disclosure
| linux/remote/[01;31m[K21[m[K934.txt

KeePass Password Safe Classic 1.29 - Crash (PoC)
| windows/dos/39[01;31m[K21[m[K6.py

Keld PHP-MySQL News Script 0.7.1 - 'login.php' SQL Injection
| php/webapps/3[01;31m[K21[m[K43.txt

Kentico CMS 7.0.75 - User Information Disclosure
| asp/webapps/3[01;31m[K21[m[K57.txt

Kerio MailServer 5.0/5.1 Web Mail - Multiple Cross-Site Scripting Vulnerabilities |
cgi/webapps/[01;31m[K21[m[K728.txt

Key Focus KF Web Server 1.0.2 - Directory Contents Disclosure
| windows/remote/[01;31m[K21[m[K597.txt

KeyHelp - ActiveX LaunchTriPane Remote Code Execution (Metasploit)
| windows/remote/[01;31m[K21[m[K888.rb

Kiasabz Article News CMS Magazine - SQL Injection
| php/webapps/1[01;31m[K21[m[K39.txt

kicq 2.0.0b1 - Invalid ICQ Packet Denial of Service
| linux/dos/[01;31m[K21[m[K262.txt

Killer Protection 1.0 - Information Disclosure
| php/webapps/[01;31m[K21[m[K912.txt

Kingsoft Antivirus/Internet Security 9+ - Local Privilege Escalation
| windows/local/434[01;31m[K21[m[K.py

Kirby CMS 2.1.0 - Cross-Site Request Forgery / Content Upload / PHP Script Execution |
php/webapps/38[01;31m[K21[m[K0.txt

Kite 1.20[01;31m[K21[m[K.610.0 - Unquoted Service Path
| windows/local/50975.txt

KiTTY Portable 0.65.0.2p (Windows 7) - Local kitty.ini Overflow (Wow64 Egghunter) |
windows/local/391[01;31m[K21[m[K.py

KMMail 1.0 - E-Mail HTML Injection
| php/webapps/[01;31m[K21[m[K956.txt

KMPlayer 2.9.3.1[01;31m[K21[m[K4 - '.ksf' Remote Buffer Overflow
| multiple/remote/35398.pl

KMPlayer 2.9.3.1[01;31m[K21[m[K4 - Multiple Remote Denial of Service Vulnerabilities |
linux/dos/30580.txt

KMPlayer 3.8.0.117 - Local Buffer Overflow
| windows/local/3[01;31m[K21[m[K52.py

Knowledge Base Enterprise Edition 4.62.0 - SQL Injection
| asp/webapps/[01;31m[K21[m[K272.txt

KnowledgeQuest 2.6 - SQL Injection
| php/webapps/54[01;31m[K21[m[K.txt

Kolibri+ Web Server 2 - GET Denial of Service
| windows/dos/96[01;31m[K21[m[K.txt

KONGA 0.14.9 - Privilege Escalation
| multiple/webapps/505[01;31m[K21[m[K.py

Konica Minolta FTP Utility 1.00 - CWD Command Overflow (SEH)
| windows/remote/39[01;31m[K21[m[K5.py

Kostenloses Linkmanagementscript - Remote File Inclusion
| php/webapps/56[01;31m[K21[m[K.txt

kr-web 1.1b2 - Remote File Inclusion
| php/webapps/10[01;31m[K21[m[K6.txt

Kronos Telestaff < 2.92EU29 - SQL Injection
| asp/webapps/4[01;31m[K21[m[K27.txt

Kshop 2.22 - 'kshop_search.php' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K90.txt

Kubeit CMS - SQL Injection
| php/webapps/1[01;31m[K21[m[K15.txt

Kubio AI Page Builder 2.5.1 - Local File Inclusion (LFI)
| multiple/webapps/5[01;31m[K21[m[K25.py

Kukol E.V. HTTP & FTP Server Suite 6.2 - File Disclosure
| windows/remote/231[01;31m[K21[m[K.txt

kusaba x 0.9.1 - Multiple Vulnerabilities
| php/webapps/172[01;31m[K21[m[K.txt

Kwintv - Local Buffer Overflow
| linux/local/2[01;31m[K21[m[K.c

k_fileManager 1.2 - 'dwl_include_path' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K04.txt

k_shoutbox 4.4 - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K03.txt

Ladder v0.0.[01;31m[K21[m[K - Server-side request forgery (SSRF)
| go/webapps/51869.txt

Lattice Semiconductor PAC-Designer 6.[01;31m[K21[m[K - '.PAC' Local Overflow | windows/local/19006.py

Lattice Semiconductor PAC-Designer 6.[01;31m[K21[m[K - Symbol Value Buffer Overflow (Metasploit) | windows/local/19175.rb

Laundry Booking Management System 1.0 - 'Multiple' SQL Injection | php/webapps/50[01;31m[K21[m[K9.txt

Laurent Adda Les Commentaires 2.0 - PHP Script 'admin.php' Remote File Inclusion | php/webapps/236[01;31m[K21[m[K.txt

Lazarus Guestbook 1.6 - 'codes-english.php?show' Cross-Site Scripting | php/webapps/28[01;31m[K21[m[K1.txt

Lazarus Guestbook 1.6 - 'picture.php?img' Cross-Site Scripting | php/webapps/28[01;31m[K21[m[K2.txt

LearnPress WordPress LMS Plugin 4.2.7 - SQL Injection | php/webapps/5[01;31m[K21[m[K71.txt

Lenovo R[01;31m[K21[m[K05 - Cross-Site Request Forgery (Command Execution) | hardware/webapps/46147.py

Leszek Krupinski L-Forum 2.4 - Search Script SQL Injection | php/webapps/[01;31m[K21[m[K708.txt

LG LR3100p 1.30 Series Router - IP Packet Flags Denial of Service | hardware/dos/[01;31m[K21[m[K736.txt

LG MRA58K - 'ASFParser::ParseHeaderExtensionObjects' Missing Bounds-Checking | android/dos/4[01;31m[K21[m[K71.txt

LG MRA58K - Missing Bounds-Checking in AVI Stream Parsing | android/dos/4[01;31m[K21[m[K70.txt

LG MRA58K - Out-of-Bounds Heap Read in CAVIFileParser::Destroy Resulting in Invalid Free | android/dos/4[01;31m[K21[m[K69.txt

libc/glob(3) - Resource Exhaustion / Remote ftpd-anonymous (Denial of Service) | multiple/dos/15[01;31m[K21[m[K5.txt

libcroco 0.6.12 - Denial of Service | linux/dos/4[01;31m[K21[m[K47.txt

```
libdbus - 'DBUS_SYSTEM_BUS_ADDRESS' Local Privilege Escalation
| linux/local/[01;31m[K21[m[K323.c

liblesstif 2-0.93.94-4mdk - 'DEBUG_FILE' Local Privilege Escalation
| linux/local/[01;31m[K21[m[K44.sh

libquicktime 1.2.4 - Denial of Service
| linux/dos/4[01;31m[K21[m[K48.txt

LibrettoCMS 2.2.2 - Arbitrary File Upload
| php/webapps/26[01;31m[K21[m[K3.txt

LibrettoCMS File Manager - Arbitrary File Upload (Metasploit)
| php/remote/264[01;31m[K21[m[K.rb

libxslt 1.1.x - RC4 Encryption and Decryption functions Buffer Overflow
| linux/remote/3[01;31m[K21[m[K33.txt

Linea[01;31m[K21[m[K 1.2.1 - 'search' Cross-Site Scripting
| php/webapps/34811.txt

LinkedIn Toolbar 3.0.2.1098 - Remote Buffer Overflow
| windows/remote/4[01;31m[K21[m[K7.html

Linkspider 1.08 - Multiple Remote File Inclusions
| php/webapps/32[01;31m[K21[m[K7.txt

Linksys BEFSR41 1.4x - 'Gozila.cgi' Denial of Service
| hardware/dos/[01;31m[K21[m[K975.txt

Linksys SPA-[01;31m[K21[m[K02 Phone Adapter Packet Handling - Denial of
Service                                          |
hardware/dos/31478.txt

Linksys WAP11 1.3/1.4 / D-Link DI-804 4.68/Dl-704 2.56 b5 - Embedded
HTTP Server Denial of Service         |
hardware/dos/[01;31m[K21[m[K978.txt

Linksys WAP55AG 1.0.7 - SNMP Community String Insecure Configuration
| hardware/remote/237[01;31m[K21[m[K.txt

Linux Kernel - 'ping' Local Denial of Service
| android/dos/4[01;31m[K21[m[K35.c

Linux Kernel 2.0.x/2.2.x/2.4.x (FreeBSD 4.x) - Network Device Driver
Frame Padding Information Disclosure  |
bsd/remote/2[01;31m[K21[m[K31.pl

Linux Kernel 2.2 - 'mmap()' Local Denial of Service
| linux/dos/2[01;31m[K21[m[K05.c
```

```
Linux Kernel 2.2.18 (RedHat 6.2/7.0 / 2.2.14/2.2.18/2.2.18ow4) -
ptrace/execve Race Condition Privilege Es |
linux/local/207[01;31m[K21[m[K.c

Linux Kernel 2.2.x/2.3/2.4.x - 'd_path()' Path Truncation
| linux/local/[01;31m[K21[m[K353.c

Linux Kernel 2.2/2.4 - Deep Symbolic Link Denial of Service
| linux/dos/[01;31m[K21[m[K122.sh

Linux Kernel 2.2/2.4 - Ptrace/Setuid Exec Privilege Escalation
| linux/local/[01;31m[K21[m[K124.txt

Linux Kernel 2.4.18/2.4.19 - Privileged File Descriptor Resource
Exhaustion (Denial of Service)            |
linux/dos/[01;31m[K21[m[K598.c

Linux Kernel 2.6.0 < 2.6.31 - 'pipe.c' Local Privilege Escalation (1)
| linux/local/333[01;31m[K21[m[K.c

Linux Kernel 2.6.[01;31m[K21[m[K.1 - IPv6 Jumbo Bug Remote Denial of
Service                                          | linux/dos/4893.c

Linux Kernel 2.6.30 - 'atalk_getname()' 8-bytes Stack Disclosure (1)
| linux/local/95[01;31m[K21[m[K.c

Linux Kernel 3.10.0-514.[01;31m[K21[m[K.2.el7.x86_64 / 3.10.0-
514.26.1.el7.x86_64 (CentOS 7) - SUID Position Independen |
linux/local/42887.c

Linux Kernel 3.3.5 - '/drivers/media/media-device.c' Local Information
Disclosure                          | linux/local/39[01;31m[K21[m[K4.c

Linux Kernel 4.4.0-[01;31m[K21[m[K (Ubuntu 16.04 x64) - Netfilter
'target_offset' Out-of-Bounds Privilege Escalation    | linux_x86-
64/local/40049.c

Linux Kernel 4.4.0-[01;31m[K21[m[K < 4.4.0-51 (Ubuntu 14.04/16.04 x64)
- 'AF_PACKET' Race Condition Privilege Escalatio | windows_x86-
64/local/47170.c

Linux Kernel < 2.6.30.5 - 'cfg80[01;31m[K21[m[K1' Remote Denial of
Service                                            | linux/dos/9442.c

Linux Kernel < 4.10.13 - 'keyctl_set_reqkey_keyring' Local Denial of
Service                                | linux/dos/4[01;31m[K21[m[K36.c

Linux Kernel < 4.4.0-[01;31m[K21[m[K (Ubuntu 16.04 x64) - 'netfilter
target_offset' Local Privilege Escalation          | linux_x86-
64/local/44300.c
```

```
Linux Kernel UDEV < 1.4.1 - 'Netlink' Local Privilege Escalation
(Metasploit)                                  |
linux/local/[01;31m[K21[m[K848.rb

Linux PolicyKit - Race Condition Privilege Escalation (Metasploit)
| linux/local/350[01;31m[K21[m[K.rb

Linuxconf 1.1.x/1.2.x - Local Environment Variable Buffer Overflow (1)
| linux/local/[01;31m[K21[m[K761.c

Linuxconf 1.1.x/1.2.x - Local Environment Variable Buffer Overflow (2)
| linux/local/[01;31m[K21[m[K762.c

Linuxconf 1.1.x/1.2.x - Local Environment Variable Buffer Overflow (3)
| linux/local/[01;31m[K21[m[K763.txt

Livefyre LiveComments Plugin - Persistent Cross-Site Scripting
| php/webapps/347[01;31m[K21[m[K.txt

Livor 2.5 - 'index.php' Cross-Site Scripting
| php/webapps/298[01;31m[K21[m[K.txt

Local Glibc Shared Library (.so) 2.11.1 - Code Execution
| multiple/local/1[01;31m[K21[m[K03.txt

LocalWEB2000 2.1.0 Standard - File Disclosure
| windows/remote/[01;31m[K21[m[K475.txt

Lockstep Backup for Workgroups 4.0.3 - Remote Buffer Overflow
(Metasploit)                                    |
windows/remote/427[01;31m[K21[m[K.rb

LogicalDOC Enterprise 7.7.4 - Root Remote Code Execution
| java/webapps/440[01;31m[K21[m[K.txt

LogoStore - 'query' SQL Injection
| php/webapps/41[01;31m[K21[m[K0.txt

Logpoint < 5.6.4 - Root Remote Code Execution
| linux/remote/4[01;31m[K21[m[K58.py

LogWatch 2.1.1/2.5 - Insecure Temporary Directory Creation
| linux/local/[01;31m[K21[m[K356.sh

Lonerunner Zeroo HTTP Server 1.5 - Remote Buffer Overflow
| linux/remote/220[01;31m[K21[m[K.sh

Longjing Technology BEMS API 1.[01;31m[K21[m[K - Remote Arbitrary File
Download                                        |
hardware/webapps/50163.txt

Look n stop - Local Denial of Service
| windows/dos/160[01;31m[K21[m[K.c
```

LookStrike Lan Manager 0.9 - Local/Remote File Inclusion
| php/webapps/51[01;31m[K21[m[K.txt

Lotus Domino 5.0.8-9 - Non-Existent NSF Database Banner Information Disclosure |
multiple/remote/[01;31m[K21[m[K996.txt

LoveCMS 1.6.2 Final - Update Settings
| php/webapps/6[01;31m[K21[m[K0.rb

LPRNG html2ps 1.0 - Remote Command Execution
| unix/remote/[01;31m[K21[m[K974.pl

Lucent 8.x - VitalNet Password Authentication Bypass
| windows/remote/[01;31m[K21[m[K203.txt

Lucent Access Point 300/600/1500 IP Services Router - Long HTTP Request Denial of Service |
hardware/dos/[01;31m[K21[m[K656.txt

Lumigent Log Explorer 3.0.1 - XP_LogAttach_SetPort Buffer Overflow
| windows/local/[01;31m[K21[m[K551.txt

Lumigent Log Explorer XP - _LogAttach_StartProf Buffer Overflow
| windows/local/[01;31m[K21[m[K550.txt

luxcal 2.7.0 - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K324.txt

LuxCal 3.2.2 - Cross-Site Request Forgery / Blind SQL Injection
| php/webapps/32[01;31m[K21[m[K1.txt

Lycos HTMLGear - guestGear CSS HTML Injection
| cgi/webapps/[01;31m[K21[m[K802.txt

Lynx 2.8.x - Command Line URL CRLF Injection
| linux/remote/[01;31m[K21[m[K722.pl

macOS - 'process_policy' Stack Leak Through Uninitialized Field
| macos/dos/435[01;31m[K21[m[K.c

Macromedia 10.1.4.20 - 'SwDir.dll' Internet Explorer Stack Overflow Denial of Service |
windows/dos/34[01;31m[K21[m[K.html

Macromedia JRun 3/4 - Administrative Authentication Bypass
| windows/remote/[01;31m[K21[m[K582.txt

Macromedia JRun 3/4 JSP Engine - Denial of Service
| windows/dos/[01;31m[K21[m[K536.jsp

Macromedia Sitespring 1.2 - Default Error Page Cross-Site Scripting
| jsp/webapps/[01;31m[K21[m[K6[01;31m[K21[m[K.txt

```
Magic Photo Storage Website - '/user/add_news.php?_config[site_path]'
Remote File Inclusion                |
php/webapps/294[01;31m[K21[m[K.txt

MagnusSolution magnusbilling 7.3.0 - Command Injection
| multiple/webapps/5[01;31m[K21[m[K70.txt

MailBee WebMail Pro 4.1 - Remote File Disclosure
| asp/webapps/49[01;31m[K21[m[K.txt

MailReader.com 2.3.x - 'NPH-MR.cgi' File Disclosure
| cgi/webapps/[01;31m[K21[m[K966.txt

MAILsweeper SMTP 4.2.1 + F-Secure Anti-Virus 5.0.2/5.2.1 - File Scanner
Malicious Archive Denial of Servic | windows/dos/[01;31m[K21[m[K006.txt

Maintain 3.0.0-RC2 - 'Example6.php' Remote File Inclusion
| php/webapps/288[01;31m[K21[m[K.txt

MakeBook 2.2 - Form Field Input Validation
| cgi/webapps/[01;31m[K21[m[K535.txt

Mambo Component CopperminePhotoGalery - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K96.txt

Mambo Component cropimage 1.0 - Remote File Inclusion
| php/webapps/2[01;31m[K21[m[K7.txt

Mambo Component MamboWiki 0.9.6 - Remote File Inclusion
| php/webapps/2[01;31m[K21[m[K3.txt

Mambo Component MMP 1.2 - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K82.txt

Mambo Component Peoplebook 1.0 - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K84.txt

Mambo Component Remository 3.25 - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K72.txt

Mambo Component SMF Forum 1.3.1.3 - Remote File Inclusion
| php/webapps/20[01;31m[K21[m[K.txt

ManageEngine ADManager Plus 5.2 Build 5[01;31m[K21[m[K0 - 'domainName'
Cross-Site Scripting                    |
java/webapps/36667.txt

ManageEngine ADManager Plus 5.2 Build 5[01;31m[K21[m[K0 - 'Operation'
Cross-Site Scripting                     |
java/webapps/36666.txt

ManageEngine OpManager - Remote Code Execution (Metasploit)
| java/remote/382[01;31m[K21[m[K.rb
```

Mandrake 7/8/9 / RedHat 6.x/7 Bonobo EFSTool - Commandline Argument Buffer Overflow (1) | linux/local/[01;31m[K21[m[K583.pl

Mandrake 7/8/9 / RedHat 6.x/7 Bonobo EFSTool - Commandline Argument Buffer Overflow (2) | linux/local/[01;31m[K21[m[K584.pl

Mandrake 7/8/9 / RedHat 6.x/7 Bonobo EFSTool - Commandline Argument Buffer Overflow (3) | linux/local/[01;31m[K21[m[K585.c

Manhali 1.8 - Local File Inclusion
| php/webapps/[01;31m[K21[m[K418.txt

Mantis Bug Tracker 0.15.x/0.16/0.17.x - JPGraph Remote File Inclusion Command Execution | php/webapps/[01;31m[K21[m[K727.txt

Mapscrn 2.03 - Local Buffer Overflow (PoC)
| linux/dos/4[01;31m[K21[m[K44.py

MASM3[01;31m[K21[m[K 11 Quick Editor '.qeditor' 4.0g - '.qse' File Buffer Overflow (SEH) (ASLR + SafeSEH Bypass) | windows/local/37799.py

Master IP CAM 01 3.3.4.[01;31m[K21[m[K03 - Remote Command Execution
| cgi/webapps/46400.py

Matt Kruse Calendar Script 2.2 - Arbitrary Command Execution
| cgi/remote/199[01;31m[K21[m[K.txt

Matu FTP 1.74 - Client Buffer Overflow
| windows/remote/[01;31m[K21[m[K410.pl

Matu FTP Server 1.13 - Remote Buffer Overflow
| windows/remote/[01;31m[K21[m[K468.pl

Max Feoktistov Small HTTP server 1.[01;31m[K21[m[K2 - Buffer Overflow
| windows/dos/20017.py

Max Network Technology BBSMAX 4.2 - 'post.aspx' Cross-Site Scripting
| asp/webapps/337[01;31m[K21[m[K.txt

Maxthon Browser 1.x - Content-Type Buffer Overflow
| windows/remote/3[01;31m[K21[m[K97.pl

Mayasan Portal 2.0 - 'haberdetay.asp' SQL Injection
| asp/webapps/144[01;31m[K21[m[K.txt

McAfee Virtual Technician (MVT) 6.5.0.[01;31m[K21[m[K01 - Insecure ActiveX Method | windows/remote/24907.txt

McAfee VirusScan 10.0.[01;31m[K21[m[K - ActiveX control Stack Overflow (PoC) |
windows/dos/3890.html

McKesson Pathways Homecare 6.5 - Weak 'Username' and Password Encryption |
windows/local/[01;31m[K21[m[K173.pl

mcNews 1.x - File Disclosure
| php/webapps/[01;31m[K21[m[K463.txt

MCPWS Personal WebServer 1.3.[01;31m[K21[m[K - Denial of Service
| windows/dos/891.pl

MD-Pro 1.083.x - Survey Module 'pollID' Blind SQL Injection
| php/webapps/90[01;31m[K21[m[K.txt

MDaemon WorldClient 5.0.x - Folder Creation Buffer Overflow
| windows/remote/[01;31m[K21[m[K439.txt

ME Download System 1.3 - 'header.php' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K22.txt

Media Player Classic (MPC) 1.5 - WebServer Request Handling Remote Denial of Service |
multiple/dos/380[01;31m[K21[m[K.pl

Media Player Classic 1.3.[01;31m[K21[m[K89.0 - 'iacenc.dll' DLL Hijacking |
windows/local/14765.c

Mediacoder 0.7.3.4672 - Local Overflow (SEH)
| windows/local/128[01;31m[K21[m[K.py

MediaInSpot CMS - Local File Inclusion (1)
| php/webapps/1[01;31m[K21[m[K41.txt

Meeting Room Booking System (MRBS) 1.2.6 - 'day.php' Cross-Site Scripting |
php/webapps/3[01;31m[K21[m[K44.txt

Meeting Room Booking System (MRBS) 1.2.6 - 'help.php' Cross-Site Scripting |
php/webapps/3[01;31m[K21[m[K49.txt

Meeting Room Booking System (MRBS) 1.2.6 - 'month.php' Cross-Site Scripting |
php/webapps/3[01;31m[K21[m[K46.txt

Meeting Room Booking System (MRBS) 1.2.6 - 'report.php' Cross-Site Scripting |
php/webapps/3[01;31m[K21[m[K48.txt

```
Meeting Room Booking System (MRBS) 1.2.6 - 'search.php' Cross-Site
Scripting                                  |
php/webapps/3[01;31m[K21[m[K47.txt

Meeting Room Booking System (MRBS) 1.2.6 - 'week.php' Cross-Site
Scripting                                   |
php/webapps/3[01;31m[K21[m[K45.txt

Melange Chat System 2.0.2 Beta 2 - '/yell' Remote Buffer Overflow
| multiple/dos/[01;31m[K21[m[K379.pl

Menasoft SPHEREserver 0.99 - Denial of Service
| multiple/dos/[01;31m[K21[m[K337.c

Mercury Audio Player 1.[01;31m[K21[m[K - '.b4s' Local Stack Overflow
| windows/local/8580.py

Mercury Audio Player 1.[01;31m[K21[m[K - '.m3u' Local Stack Overflow
| windows/local/8583.py

Mercury Audio Player 1.[01;31m[K21[m[K - '.m3u' Local Stack Overflow
(PoC)                                                  |
windows/dos/8578.pl

Mercury Audio Player 1.[01;31m[K21[m[K - '.pls' Overwrite
(SEH)                                                                |
windows/local/8582.py

Mercury/32 Mail SMTPD - AUTH CRAM-MD5 Buffer Overflow (Metasploit)
| windows/remote/168[01;31m[K21[m[K.rb

Merit AAA RADIUS Server 3.8 - rlmadmin Symbolic Link
| unix/local/[01;31m[K21[m[K101.sh

Messagerie 1.0 - Arbitrary User Removal Denial of Service
| php/dos/[01;31m[K21[m[K428.txt

Metasploit < 4.4 - pcap_log Plugin Privilege Escalation (Metasploit)
| multiple/remote/[01;31m[K21[m[K927.rb

Mewsoft NetAuction 3.0 - Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K553.txt

Michael Schatz Books 0.54/0.6 PostNuke Module - Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K903.txt

Micro Focus Cobol 4.1 - Arbitrary Command Execution
| unix/local/206[01;31m[K21[m[K.txt

Micro Focus Filr 2 2.0.0.4[01;31m[K21[m[K/1.2 1.2.0.846 - Multiple
Vulnerabilities                                          |
java/webapps/40161.txt
```

```
Micro Focus Filr 3.4.0.[01;31m[K21[m[K7 - Path Traversal / Local
Privilege Escalation                                    |
linux/webapps/46450.txt

Microchip TimeProvider 4100 (Configuration modules) 2.4.6 - OS Command
Injection                              |
hardware/remote/5[01;31m[K21[m[K19.NA

Microchip TimeProvider 4100 Grandmaster (Banner Config Modules) 2.4.6 -
Stored Cross-Site Scripting (XSS)  |
hardware/remote/5[01;31m[K21[m[K20.NA

Microchip TimeProvider 4100 Grandmaster (Data plot modules) 2.4.6 - SQL
Injection                              |
hardware/remote/5[01;31m[K21[m[K22.NA

Micropoint ProActive Denfense 'Mp110013.sys' 1.3.10123.0 - Local
Privilege Escalation                        |
windows/local/12[01;31m[K21[m[K3.c

Microsoft ASP.NET - Padding Oracle (MS10-070)
| asp/remote/15[01;31m[K21[m[K3.pl

Microsoft Content Management Server 2001 - Cross-Site Scripting
| asp/webapps/[01;31m[K21[m[K920.txt

Microsoft Edge Chakra JIT - 'DictionaryPropertyDescriptor::CopyFrom'
Type Confusion                          |
windows/dos/45[01;31m[K21[m[K5.js

Microsoft Edge Chakra JIT - 'InlineArrayPush' Type Confusion
| windows/dos/45[01;31m[K21[m[K6.js

Microsoft Edge Chakra JIT - ImplicitCallFlags Check Bypass with Intl
| windows/dos/45[01;31m[K21[m[K3.js

Microsoft Edge Chakra JIT - InitializeNumberFormat and
InitializeDateTimeFormat Type Confusion             |
windows/dos/45[01;31m[K21[m[K7.js

Microsoft Edge Chakra JIT - Parameter Scope Parsing Type Confusion
| windows/dos/45[01;31m[K21[m[K4.js

Microsoft Excel 2000/2003 - Sheet Name (PoC)
| windows/dos/41[01;31m[K21[m[K.txt

Microsoft Excel 2007 - '.xlb' Local Buffer Overflow (MS11-
0[01;31m[K21[m[K) (Metasploit)                                  |
windows/local/18087.rb

Microsoft Excel 2007 SP2 - Buffer Overwrite (MS11-0[01;31m[K21[m[K)
| windows/local/18067.txt
```

Microsoft Excel 2007/2010/2013 - BIFFRecord Use-After-Free
| windows/dos/38[01;31m[K21[m[K4.txt

Microsoft Exchange 2019 15.2.2[01;31m[K21[m[K.12 - Authenticated Remote Code Execution |
windows/remote/48153.py

Microsoft Exchange Active Directory Topology 15.02.1118.007 - 'Service MSExchangeADTopology' Unquoted Serv |
windows/local/51[01;31m[K21[m[K2.txt

Microsoft Exchange Server - Remote Code Execution (MS05-0[01;31m[K21[m[K) |
windows/remote/947.pl

Microsoft Foundation Class Library 7.0 - ISAPI Buffer Overflow
| windows/remote/[01;31m[K21[m[K601.c

Microsoft FrontPage Server Extensions - 'fp30reg.dll' (MS03-051)
| windows/remote/1[01;31m[K21[m[K.c

Microsoft GamingServices 2.47.10001.0 - 'GamingServices' Unquoted Service Path |
windows/local/49[01;31m[K21[m[K4.txt

Microsoft Host Integration Server 2004-2010 - Remote Denial of Service
| windows/dos/36[01;31m[K21[m[K1.txt

Microsoft HTML Help Workshop 4.74 - '.hhp' Local Buffer Overflow (1)
| windows/local/103[01;31m[K21[m[K.py

Microsoft IIS 4.0/5.0 - Chunked Encoding Transfer Heap Overflow (1)
| windows/remote/[01;31m[K21[m[K368.c

Microsoft IIS 4.0/5.0 - Chunked Encoding Transfer Heap Overflow (2)
| windows/remote/[01;31m[K21[m[K369.c

Microsoft IIS 4.0/5.0 - Chunked Encoding Transfer Heap Overflow (3)
| windows/remote/[01;31m[K21[m[K370.c

Microsoft IIS 4.0/5.0 - Chunked Encoding Transfer Heap Overflow (4)
| windows/remote/[01;31m[K21[m[K371.c

Microsoft IIS 4.0/5.0 - HTTP Error Page Cross-Site Scripting
| windows/remote/[01;31m[K21[m[K372.txt

Microsoft IIS 4.0/5.0 - SMTP Service Encapsulated SMTP Address (MS99-027) |
windows/remote/[01;31m[K21[m[K613.txt

Microsoft IIS 4.0/5.0 - SSI Buffer Overrun Privilege Escalation
| windows/local/[01;31m[K21[m[K071.c

Microsoft IIS 4.0/5.0/5.1 - Authentication Method Disclosure
| windows/remote/[01;31m[K21[m[K313.txt

Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network Name Disclosure |
windows/remote/[01;31m[K21[m[K057.txt

Microsoft IIS 5.0 - 'CodeBrws.asp' Source Code Disclosure
| windows/remote/[01;31m[K21[m[K385.txt

Microsoft IIS 5.0 - False Content-Length Field Denial of Service
| windows/dos/[01;31m[K21[m[K177.txt

Microsoft IIS 5.0 - IDC Extension Cross-Site Scripting
| windows/remote/[01;31m[K21[m[K910.txt

Microsoft IIS 5.0 - In-Process Table Privilege Escalation
| windows/local/[01;31m[K21[m[K072.txt

Microsoft Index Server 2.0 - File Information / Full Path Disclosure
| windows/remote/[01;31m[K21[m[K113.txt

Microsoft Internet Explorer - 'MDAC' Remote Code Execution (MS06-014) (Metasploit) (2) |
windows/remote/[01;31m[K21[m[K64.pm

Microsoft Internet Explorer - execCommand Use-After-Free (MS12-063) (Metasploit) |
windows/remote/[01;31m[K21[m[K840.rb

Microsoft Internet Explorer 3/4/5 / Netscape Communicator 4 - IMG Tag Denial of Service |
multiple/dos/[01;31m[K21[m[K041.txt

Microsoft Internet Explorer 4/5/6 - XML Datasource Applet File Disclosure |
windows/local/[01;31m[K21[m[K7[01;31m[K21[m[K.html

Microsoft Internet Explorer 5 - Cascading Style Sheet File Disclosure (MS02-023) |
windows/remote/[01;31m[K21[m[K361.txt

Microsoft Internet Explorer 5 - Dialog Same Origin Policy Bypass Variant (MS02-047) |
windows/remote/[01;31m[K21[m[K750.txt

Microsoft Internet Explorer 5 - Document Reference Zone Bypass
| windows/remote/[01;31m[K21[m[K883.html

Microsoft Internet Explorer 5 - IFrame/Frame Cross-Site/Zone Script Execution |
windows/remote/[01;31m[K21[m[K777.txt

Microsoft Internet Explorer 5 - JavaScript Local File Enumeration (1)
| windows/remote/[01;31m[K21[m[K198.html

Microsoft Internet Explorer 5 - JavaScript Local File Enumeration (2)
| windows/remote/[01;31m[K21[m[K199.txt

Microsoft Internet Explorer 5 - Zone Spoofing (MS01-055)
| windows/remote/[01;31m[K21[m[K118.txt

Microsoft Internet Explorer 5.0.1 - Wildcard DNS Cross-Site Scripting
| windows/remote/24[01;31m[K21[m[K3.txt

Microsoft Internet Explorer 5.0.1/6.0 - Content-Disposition Handling
File Execution |
windows/remote/[01;31m[K21[m[K452.txt

Microsoft Internet Explorer 5.0/4.0.1 - hhopen OLE Control Buffer
Overflow |
windows/remote/195[01;31m[K21[m[K.txt

Microsoft Internet Explorer 5.5/6.0 - History List Script Injection
| windows/remote/[01;31m[K21[m[K376.html

Microsoft Internet Explorer 5.5/6.0 - Spoofable File Extensions
| windows/remote/[01;31m[K21[m[K164.txt

Microsoft Internet Explorer 5/6 - Cached Objects Zone Bypass
| windows/remote/[01;31m[K21[m[K959.txt

Microsoft Internet Explorer 5/6 - Cookie Disclosure/Modification
| windows/remote/[01;31m[K21[m[K144.txt

Microsoft Internet Explorer 5/6 - CSSText Bold Font Denial of Service
| windows/dos/[01;31m[K21[m[K556.txt

Microsoft Internet Explorer 5/6 - FTP Web View Cross-Site Scripting
| windows/remote/[01;31m[K21[m[K515.txt

Microsoft Internet Explorer 5/6 - GetObject File Disclosure
| windows/remote/[01;31m[K21[m[K195.txt

Microsoft Internet Explorer 5/6 - JavaScript Interface Spoofing
| windows/remote/[01;31m[K21[m[K127.txt

Microsoft Internet Explorer 5/6 - OBJECT Tag Same Origin Policy
Violation |
windows/remote/[01;31m[K21[m[K606.txt

Microsoft Internet Explorer 5/6 - Recursive JavaScript Event Denial of
Service |
windows/dos/[01;31m[K21[m[K416.txt

Microsoft Internet Explorer 5/6 - Self-Referential Object Denial of Service |
windows/dos/[01;31m[K21[m[K404.html

Microsoft Internet Explorer 5/6 - Unauthorized Document Object Model Access |
windows/remote/[01;31m[K21[m[K940.txt

Microsoft Internet Explorer 5/6 - XML Redirect File Disclosure
| windows/remote/[01;31m[K21[m[K749.txt

Microsoft Internet Explorer 5/6 / Konqueror 2.2.2/3.0 / Weblogic Server 5/6/7 - Invalid X.509 Certificate |
windows/remote/[01;31m[K21[m[K692.txt

Microsoft Internet Explorer 5/6 / Microsoft ISA Server 2000 / Microsoft Proxy Server 2.0 Gopher Client - R |
windows/remote/[01;31m[K21[m[K510.pl

Microsoft Internet Explorer 5/6 / Mozilla 0.8/0.9.x / Opera 5/6 - JavaScript Interpreter Denial of Service |
windows/dos/[01;31m[K21[m[K346.html

Microsoft Internet Explorer 5/6 / Outlook 2000/2002/5.5 / Word 2000/2002 - VBScript ActiveX Word Object De |
windows/dos/[01;31m[K21[m[K366.txt

Microsoft Internet Explorer 5/6 Legacy Text Formatting - ActiveX Component Buffer Overflow |
windows/remote/[01;31m[K21[m[K748.txt

Microsoft Internet Explorer 6 - Absolute Position Block Denial of Service |
windows/dos/23[01;31m[K21[m[K5.html

Microsoft Internet Explorer 6 - File Attachment Script Execution
| windows/remote/[01;31m[K21[m[K705.txt

Microsoft Internet Explorer 6 - HREF Save As Denial of Service
| windows/dos/24[01;31m[K21[m[K1.txt

Microsoft Internet Explorer 6 - Multiple COM Object Color Property Denial of Service Vulnerabilities |
windows/dos/284[01;31m[K21[m[K.html

Microsoft Internet Explorer 6 - RevealTrans Denial of Service
| windows/dos/28[01;31m[K21[m[K3.txt

Microsoft Internet Explorer 6 - URI Handler Restriction Circumvention
| windows/remote/[01;31m[K21[m[K803.txt

Microsoft Internet Explorer 6 < 10 - Mouse Tracking
| windows/remote/233[01;31m[K21[m[K.txt

Microsoft Internet Explorer 6.0 / Mozilla 0.9.6 / Opera 5.1 - Image Count Denial of Service | multiple/dos/[01;31m[K21[m[K181.txt

Microsoft Internet Explorer 6/7 - CSS Handling Denial of Service | windows/dos/10[01;31m[K21[m[K0.txt

Microsoft Internet Explorer 6/7/8 - Memory Corruption | windows/remote/154[01;31m[K21[m[K.html

Microsoft Internet Explorer 8/9/10/11 / IIS / CScript.exe/WScript.exe VBScript - CRegExp..Execute Use of U | windows/remote/407[01;31m[K21[m[K.html

Microsoft Internet Explorer 9 - Cross-Site Scripting Filter Bypass | windows/dos/2[01;31m[K21[m[K00.txt

Microsoft Internet Explorer 9 - IEFRAME CView::EnsureSize Use-After-Free (MS13-0[01;31m[K21[m[K) | windows/dos/40935.html

Microsoft Internet Explorer/Opera - Source Code viewer Null Character Handling | windows/remote/1[01;31m[K21[m[K56.txt

Microsoft MSN Messenger 1 < 4 - Malformed Invite Request Denial of Service | windows/dos/[01;31m[K21[m[K481.txt

Microsoft NetMeeting 2.1/3.0.1 4.4.3385 - CALLTO URL Buffer Overflow (PoC) | windows/dos/226[01;31m[K21[m[K.txt

Microsoft Office 2007 - 'OGL.dll' ValidateBitmapInfo Bounds Check Failure (MS15-097) | windows/dos/38[01;31m[K21[m[K7.txt

Microsoft Office 2007 - BIFFRecord Length Use-After-Free | windows/dos/38[01;31m[K21[m[K5.txt

Microsoft Office 2007 - OLESSDirectyEntry.CreateTime Type Confusion | windows/dos/38[01;31m[K21[m[K6.txt

Microsoft Office 2007/2010 - OLE Arbitrary Command Execution | windows/local/35[01;31m[K21[m[K6.py

Microsoft Office 2019 MSO Build 1808 - NTLMv2 Hash Disclosure | windows/remote/5[01;31m[K21[m[K13.NA

Microsoft Outlook 98/2000/2002 - Arbitrary Code Execution | windows/remote/[01;31m[K21[m[K004.txt

Microsoft Outlook 98/2000/2002 - Unauthorized Email Access
| windows/remote/[01;31m[K21[m[K003.txt

Microsoft Outlook Express 5.5 - Denial of Service Device Denial of Service |
windows/dos/[01;31m[K21[m[K419.txt

Microsoft Outlook Express 5.5/6.0 - S/MIME Buffer Overflow
| windows/remote/[01;31m[K21[m[K932.pl

Microsoft Outlook Express 5/6 - MHTML URL Handler File Rendering
| windows/remote/[01;31m[K21[m[K711.html

Microsoft Outlook Express 5/6 - Spoofable File Extensions
| windows/remote/[01;31m[K21[m[K631.txt

Microsoft Outlook Express 6 - '.XML' File Attachment Script Execution
| windows/remote/[01;31m[K21[m[K662.txt

Microsoft People 10.1807.[01;31m[K21[m[K31.0 - Denial of service (PoC)
| windows_x86-64/dos/45335.txt

Microsoft Pocket Internet Explorer 3.0 - Denial of Service
| windows/dos/2[01;31m[K21[m[K19.html

Microsoft Site Server 3.0 - Cross-Site Scripting
| windows/remote/[01;31m[K21[m[K260.txt

Microsoft SQL 2000/7.0 - Agent Jobs Privilege Escalation
| windows/remote/[01;31m[K21[m[K718.txt

Microsoft SQL Server 2000 - 'SQLXML' Buffer Overflow (PoC)
| windows/dos/[01;31m[K21[m[K540.txt

Microsoft SQL Server 2000 - Database Consistency Checkers Buffer Overflow |
windows/remote/[01;31m[K21[m[K650.txt

Microsoft SQL Server 2000 - Password Encrypt procedure Buffer Overflow
| windows/local/[01;31m[K21[m[K549.txt

Microsoft SQL Server 2000 - Resolution Service Heap Overflow
| windows/remote/[01;31m[K21[m[K652.cpp

Microsoft SQL Server 2000 - sp_MScopyscript SQL Injection
| windows/remote/[01;31m[K21[m[K651.txt

Microsoft SQL Server 2000 - SQLXML Script Injection
| windows/remote/[01;31m[K21[m[K541.txt

Microsoft SQL Server 2000 - User Authentication Remote Buffer Overflow
| windows/remote/[01;31m[K21[m[K693.nasl

Microsoft SQL Server 2000 / Microsoft Jet 4.0 Engine - Unicode Buffer Overflow (PoC) | windows/dos/[01;31m[K21[m[K569.txt

Microsoft Visio 2016 16.0.4738.1000 - 'Log in accounts' Denial of Service | windows/dos/466[01;31m[K21[m[K.py

Microsoft VM 2000/3000/3100/3188/3200/3300/3802/3805 series - JDBC Class Code Execution | windows/remote/[01;31m[K21[m[K808.txt

Microsoft Windows - '.png' IHDR Block Denial of Service (PoC) (1) | windows/dos/[01;31m[K21[m[K94.pl

Microsoft Windows - '.png' IHDR Block Denial of Service (PoC) (2) | windows/dos/2[01;31m[K21[m[K0.c

Microsoft Windows - '0x224000 IOCTL (WmiQueryAllData)' Kernel WMIDataDevice Pool Memory Disclosure | windows/dos/42[01;31m[K21[m[K3.cpp

Microsoft Windows - 'AfdJoinLeaf' Local Privilege Escalation (MS11-080) (Metasploit) | windows/local/[01;31m[K21[m[K844.rb

Microsoft Windows - 'ATMFD.dll' CFF table (ATMFD+0x3440b / ATMFD+0x3440e) Invalid Memory Access | windows/dos/379[01;31m[K21[m[K.txt

Microsoft Windows - 'ATMFD.dll' CharString Stream Out-of-Bounds Reads (MS15-0[01;31m[K21[m[K) | windows/dos/37923.txt

Microsoft Windows - 'IOCTL 0x390400_ operation code 0x00020000' Kernel KsecDD Pool Memory Disclosure | windows/dos/42[01;31m[K21[m[K1.cpp

Microsoft Windows - 'IOCTL_DISK_GET_DRIVE_GEOMETRY_EX' Kernel partmgr Pool Memory Disclosure | windows/dos/42[01;31m[K21[m[K6.cpp

Microsoft Windows - 'IOCTL_DISK_GET_DRIVE_LAYOUT_EX' Kernel partmgr Pool Memory Disclosure | windows/dos/42[01;31m[K21[m[K7.cpp

Microsoft Windows - 'IOCTL_MOUNTMGR_QUERY_POINTS' Kernel Mountmgr Pool Memory Disclosure | windows/dos/42[01;31m[K21[m[K2.cpp

```
Microsoft Windows - 'IOCTL_VOLUME_GET_VOLUME_DISK_EXTENTS' volmgr Pool
Memory Disclosure                    |
windows/dos/42[01;31m[K21[m[K5.cpp

Microsoft Windows - 'Jolt2.c' Denial of Service (MS00-029)
| windows/dos/[01;31m[K21[m[K4.c

Microsoft Windows - 'nt!NtNotifyChangeDirectoryFile' Kernel Pool Memory
Disclosure                          | windows/dos/42[01;31m[K21[m[K9.cpp

Microsoft Windows - 'nt!NtQueryVolumeInformationFile
(FileFsVolumeInformation)' Kernel Pool Memory Disclos |
windows/dos/42[01;31m[K21[m[K8.cpp

Microsoft Windows - 'win32k!NtGdiEnumFonts' Kernel Pool Memory
Disclosure                                    |
windows/dos/42[01;31m[K21[m[K4.txt

Microsoft Windows - 'win32k!NtGdiGetOutlineTextMetricsInternalW' Kernel
Pool Memory Disclosure              | windows/dos/42[01;31m[K21[m[K0.cpp

Microsoft Windows - Escalate Service Permissions Privilege Escalation
(Metasploit)                          |
windows/local/[01;31m[K21[m[K994.rb

Microsoft Windows - Escalate UAC Execute RunAs (Metasploit)
| windows/local/[01;31m[K21[m[K843.rb

Microsoft Windows - Escalate UAC Protection Bypass (Metasploit)
| windows/local/[01;31m[K21[m[K845.rb

Microsoft Windows - GDI (EMR_COLORMATCHTOTARGETW) (MS08-
0[01;31m[K21[m[K)                                                    |
windows/remote/6656.txt

Microsoft Windows - GDI Image Parsing Stack Overflow (MS08-
0[01;31m[K21[m[K)                                                  |
windows/local/5442.cpp

Microsoft Windows - NetpIsRemote() Remote Overflow (MS06-040)
(Metasploit)                                  |
windows/remote/[01;31m[K21[m[K62.pm

Microsoft Windows - NTUserMessageCall Win32k Kernel Pool Overflow
'schlamperei.x86.dll' (MS13-053) (Metasp |
windows_x86/local/33[01;31m[K21[m[K3.rb

Microsoft Windows - Running Object Table Register
ROTFLAGS_ALLOWANYCLIENT Privilege Escalation             |
windows/dos/420[01;31m[K21[m[K.txt
```

Microsoft Windows - UAC Protection Bypass via FodHelper Registry Key (Metasploit) | windows/local/4[01;31m[K21[m[K42.rb

Microsoft Windows 10 (1903/1909) - 'SMBGhost' SMB3.1.1 'SMB2_COMPRESSION_CAPABILITIES' Buffer Overflow (Po | windows/dos/48[01;31m[K21[m[K6.md

Microsoft Windows 7 (x86/x64) - Group Policy Privilege Escalation (MS16-072) | windows/local/40[01;31m[K21[m[K9.txt

Microsoft Windows 95/98/2000/NT 4.0 - WinHlp Item Buffer Overflow | windows/remote/[01;31m[K21[m[K485.txt

Microsoft Windows 98 - ARP Denial of Service | windows/dos/[01;31m[K21[m[K040.txt

Microsoft Windows 98/XP/ME - UPnP NOTIFY Buffer Overflow (1) | windows/remote/[01;31m[K21[m[K188.c

Microsoft Windows 98/XP/ME - UPnP NOTIFY Buffer Overflow (2) | windows/remote/[01;31m[K21[m[K189.c

Microsoft Windows Explorer - '.GIF' Image Denial of Service | windows/dos/4[01;31m[K21[m[K5.pl

Microsoft Windows FTP Server 1.4 - Authentication Bypass | windows/remote/1[01;31m[K21[m[K19.pl

Microsoft Windows Kernel - '.ANI' File Parsing Crash | windows/dos/7[01;31m[K21[m[K.html

Microsoft Windows Live Messenger 2009 - ActiveX Heap Overflow (PoC) | windows/dos/11[01;31m[K21[m[K4.html

Microsoft Windows Media Encoder 9 - 'wmex.dll' ActiveX Buffer Overflow (MS08-053) (Metasploit) | windows/remote/165[01;31m[K21[m[K.rb

Microsoft Windows Media Player 10 - '.avi' Integer Division By Zero Crash (PoC) | windows/dos/[01;31m[K21[m[K986.pl

Microsoft Windows Media Player 11.0.57[01;31m[K21[m[K.5145 - '.avi' Buffer Overflow | windows/dos/35553.pl

Microsoft Windows Media Player 11.0.57[01;31m[K21[m[K.5145 - '.mpg' Buffer Overflow | windows/dos/11531.pl

Microsoft Windows Media Player 11.0.57[01;31m[K21[m[K.5230 - Memory Corruption (PoC) | windows/dos/32477.py

Microsoft Windows Media Player 11.0.57[01;31m[K21[m[K.5262 - Remote Denial of Service | windows/dos/18271.py

Microsoft Windows Media Player 6/7 - Filename Buffer Overflow | windows/remote/[01;31m[K21[m[K670.txt

Microsoft Windows NT 3/4.0 - CSRSS Memory Access Violation | windows/local/[01;31m[K21[m[K130.c

Microsoft Windows NT 4.0 - NT4ALL Denial of Service | windows/dos/[01;31m[K21[m[K047.txt

Microsoft Windows NT 4.0/2000 - NTFS File Hiding | linux/local/[01;31m[K21[m[K258.bat

Microsoft Windows NT 4.0/2000 - Process Handle Local Privilege Escalation | windows/local/[01;31m[K21[m[K344.txt

Microsoft Windows NT 4.0/2000 - TCP Stack Denial of Service (1) | windows/dos/[01;31m[K21[m[K245.c

Microsoft Windows NT 4.0/2000 - TCP Stack Denial of Service (2) | windows/dos/[01;31m[K21[m[K246.c

Microsoft Windows NT 4.0/4.0 SP1/4.0 SP2/4.0 SP3/4.0 SP4/4.0 SP5 - RAS Phonebook Buffer Overflow | windows/local/19[01;31m[K21[m[K1.c

Microsoft Windows NT/2000 - Terminal Server Service RDP Denial of Service | windows/dos/[01;31m[K21[m[K123.txt

Microsoft Windows Server 2000 - Internet Key Exchange Denial of Service (1) | windows/dos/[01;31m[K21[m[K171.c

Microsoft Windows Server 2000 - Internet Key Exchange Denial of Service (2) | windows/dos/[01;31m[K21[m[K172.pl

Microsoft Windows Server 2000 - Lanman Denial of Service (1) | windows/dos/[01;31m[K21[m[K388.c

Microsoft Windows Server 2000 - Lanman Denial of Service (2) | windows/dos/[01;31m[K21[m[K389.txt

Microsoft Windows Server 2000 - RunAs Service Denial of Service | windows/dos/[01;31m[K21[m[K099.c

Microsoft Windows Server 2000 - RunAs Service Named Pipe Hijacking
| windows/local/[01;31m[K21[m[K069.c

Microsoft Windows XP - '.Manifest' Denial of Service
| windows/dos/[01;31m[K21[m[K240.txt

Microsoft Windows XP - HCP URI Handler Abuse
| windows/remote/[01;31m[K21[m[K717.txt

Microsoft Windows XP/2000 - Fontview Denial of Service
| windows/dos/2[01;31m[K21[m[K32.txt

Microsoft Windows XP/2000 - GDI Denial of Service
| windows/dos/[01;31m[K21[m[K131.txt

Microsoft Windows XP/2000 - PostThreadMessage() Arbitrary Process Killing |
windows/local/23[01;31m[K21[m[K0.c

Microsoft Windows XP/2000/NT 4.0 - Help Facility ActiveX Control Buffer Overflow |
windows/remote/[01;31m[K21[m[K902.c

Microsoft Windows XP/2000/NT 4.0 - Locator Service Buffer Overflow
| windows/remote/2[01;31m[K21[m[K94.txt

Microsoft Windows XP/2000/NT 4.0 - NetDDE Privilege Escalation (1)
| windows/local/[01;31m[K21[m[K922.c

Microsoft Windows XP/2000/NT 4.0 - NetDDE Privilege Escalation (2)
| windows/local/[01;31m[K21[m[K923.c

Microsoft Windows XP/2000/NT 4.0 - Network Share Provider SMB Request Buffer Overflow (1) | windows/dos/[01;31m[K21[m[K746.c

Microsoft Windows XP/2000/NT 4.0 - Network Share Provider SMB Request Buffer Overflow (2) |
windows/dos/[01;31m[K21[m[K747.txt

Microsoft Windows XP/2000/NT 4.0 - RPC Service Denial of Service (1)
| windows/dos/[01;31m[K21[m[K951.c

Microsoft Windows XP/2000/NT 4.0 - RPC Service Denial of Service (2)
| windows/dos/[01;31m[K21[m[K952.c

Microsoft Windows XP/2000/NT 4.0 - RPC Service Denial of Service (3)
| windows/dos/[01;31m[K21[m[K953.txt

Microsoft Windows XP/2000/NT 4.0 - RPC Service Denial of Service (4)
| windows/dos/[01;31m[K21[m[K954.txt

Microsoft Windows XP/2000/NT 4.0 - Window Message Subsystem Design Error (1) |
windows/local/[01;31m[K21[m[K684.c

Microsoft Windows XP/2000/NT 4.0 - Window Message Subsystem Design Error (2) |
windows/local/[01;31m[K21[m[K685.c

Microsoft Windows XP/2000/NT 4.0 - Window Message Subsystem Design Error (3) |
windows/local/[01;31m[K21[m[K686.c

Microsoft Windows XP/2000/NT 4.0 - Window Message Subsystem Design Error (4) |
windows/local/[01;31m[K21[m[K687.c

Microsoft Windows XP/2000/NT 4.0 - Window Message Subsystem Design Error (5) |
windows/local/[01;31m[K21[m[K688.c

Microsoft Windows XP/2000/NT 4.0 - Window Message Subsystem Design Error (6) |
windows/local/[01;31m[K21[m[K689.c

Microsoft Windows XP/2000/NT 4.0 - Window Message Subsystem Design Error (7) |
windows/local/[01;31m[K21[m[K690.txt

Microsoft Windows XP/2000/NT 4.0 - Window Message Subsystem Design Error (8) |
windows/local/[01;31m[K21[m[K691.txt

Microsoft Word 2010 - Crash (PoC)
| windows/dos/22[01;31m[K21[m[K5.txt

Microsoft Word 95/97/98/2000/2002 - 'INCLUDEPICTURE' Document Sharing File Disclosure |
windows/remote/[01;31m[K21[m[K812.txt

Microsoft Word 95/97/98/2000/2002 / Excel 2002 - INCLUDETEXT Document Sharing File Disclosure |
windows/remote/[01;31m[K21[m[K764.txt

Microsoft Word 97/98/2002 - Malformed Document Denial of Service
| windows/dos/23[01;31m[K21[m[K6.txt

Microsoft Xbox One 10.0.14393.[01;31m[K21[m[K52 - Code Execution (PoC)
| hardware/local/44644.txt

Midicart ASP - Remote Customer Information Retrieval
| asp/webapps/[01;31m[K21[m[K702.txt

```
Midicart PHP - Arbitrary File Upload
| php/webapps/[01;31m[K21[m[K896.txt

Midicart PHP - Information Disclosure
| php/webapps/[01;31m[K21[m[K894.txt

MiladWorkShop VIP System 1.0 - 'lang' SQL Injection
| php/webapps/48[01;31m[K21[m[K8.txt

MilleGPG5 5.7.2 Luglio 20[01;31m[K21[m[K - Local Privilege Escalation
| windows/local/50558.txt

Minerva 2.0.[01;31m[K21[m[K build 238a - 'phpbb_root_path' File
Inclusion                                                 |
php/webapps/2429.txt

miniature java Web server 1.71 - Multiple Vulnerabilities
| multiple/remote/1[01;31m[K21[m[K14.txt

MiniBB 1.2 - Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K427.txt

MiniBB RSS 2.0 Plugin - Multiple Remote File Inclusions
| php/webapps/3[01;31m[K21[m[K23.txt

MiniCMS 1.1 - Cross Site Scripting (XSS)
| php/webapps/5[01;31m[K21[m[K75.txt

miniPortail 2.2 - Cross-Site Scripting / Local File Inclusion
| php/webapps/68[01;31m[K21[m[K.txt

MiniWebsvr 0.0.9a - Remote Directory Traversal
| windows/remote/5[01;31m[K21[m[K2.py

Minix 3.1.2a - Psuedo Terminal Denial of Service
| linux/dos/3[01;31m[K21[m[K12.txt

Mirabilis ICQ 2002 - Sound Scheme Remote Configuration Modification
| windows/remote/[01;31m[K21[m[K618.txt

MIRC 2.x/3.x/4.x/5.x - Nick Buffer Overflow
| windows/remote/[01;31m[K21[m[K274.c

mIRC 6.0 - Scripting ASCTime Buffer Overflow
| windows/remote/[01;31m[K21[m[K759.txt

MIT PGP Public Key Server 0.9.2/0.9.4 - Search String Remote Buffer
Overflow                                |
linux/dos/[01;31m[K21[m[K482.txt

Mitra Informatika Solusindo cart - SQL Injection
| php/webapps/5[01;31m[K21[m[K4.txt
```

```
MJGUEST 6.8 - 'Guestbook.js.php' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K28.txt

MM 1.0.x/1.1.x - Shared Memory Library Temporary File Privilege
Escalation                                  |
linux/local/[01;31m[K21[m[K667.c

MMHAQ CMS - SQL Injection
| php/webapps/1[01;31m[K21[m[K34.txt

Mobile Atlas Creator 1.9.12 - Persistent Command Injection
| multiple/webapps/266[01;31m[K21[m[K.txt

MobileCartly 1.0 - Arbitrary File Creation (Metasploit)
| php/webapps/[01;31m[K21[m[K079.rb

MobileShop master v1.0 - SQL Injection Vuln.
| php/webapps/519[01;31m[K21[m[K.txt

Mobius DocumentDirect for the Internet 1.2 - Remote Buffer Overflow
| windows/remote/20[01;31m[K21[m[K1.c

MobPartner Chat - Multiple SQL Injections
| php/webapps/113[01;31m[K21[m[K.txt

ModernBill 1.6 - 'config.php' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K27.txt

Mojo Mail 2.7 - Email Form Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K962.txt

Mole Group Hotel Script 1.0 - SQL Injection
| php/webapps/60[01;31m[K21[m[K.txt

MoneyFlux 1.0 - 'id' SQL Injection
| php/webapps/46[01;31m[K21[m[K1.txt

Monkey HTTP Server 0.1.4 - File Disclosure
| linux/remote/[01;31m[K21[m[K857.pl

Monkey HTTP Server 0.1/0.4/0.5 - Multiple Cross-Site Scripting
Vulnerabilities                             |
multiple/remote/[01;31m[K21[m[K880.txt

Monkey HTTP Server 0.4/0.5 - Invalid POST Denial of Service
| windows/dos/[01;31m[K21[m[K981.txt

Morcego CMS 1.7.6 - Blind SQL Injection
| php/webapps/91[01;31m[K21[m[K.php

Mountain Network Systems WebCart 8.4 - Command Execution
| cgi/remote/[01;31m[K21[m[K125.pl
```

Movable Type 4.2x/4.3x - Web Upgrade Remote Code Execution (Metasploit)
| multiple/remote/243[01;31m[K21[m[K.rb

Movable Type Pro 5.13en - Persistent Cross-Site Scripting
| php/webapps/2[01;31m[K21[m[K51.txt

Movie Rating System 1.0 - Broken Access Control (Admin Account
Creation) (Unauthenticated) |
php/webapps/506[01;31m[K21[m[K.py

Mozilla 0.9.x/1.0 - JavaScript URL Host Spoofing Arbitrary Cookie
Access |
multiple/remote/[01;31m[K21[m[K638.txt

Mozilla 1.0/1.1 - FTP View Cross-Site Scripting
| unix/remote/[01;31m[K21[m[K682.txt

Mozilla Bonsai - Multiple Cross-Site Scripting Vulnerabilities
| cgi/webapps/[01;31m[K21[m[K729.txt

Mozilla Bonsai 1.3 - Full Path Disclosure
| cgi/webapps/[01;31m[K21[m[K730.txt

Mozilla Firefox 3.0.7 - OnbeforeUnLoad DesignMode Dereference Crash
| multiple/dos/8[01;31m[K21[m[K9.html

Mozilla Firefox 3.5 - 'Font tags' Remote HeapSpray (2)
| windows/remote/9[01;31m[K21[m[K4.pl

Mozilla Firefox 3.6.8 - 'Math.random()' Cross Domain Information
Disclosure |
unix/remote/346[01;31m[K21[m[K.c

Mozilla Suite/Firefox/Thunderbird - Nested Anchor Tag Status Bar
Spoofing |
linux/remote/252[01;31m[K21[m[K.txt

Mp3 MuZik - Database Disclosure
| asp/webapps/1[01;31m[K21[m[K97.txt

Mp3 Online Id Tag Editor - Remote File Inclusion
| php/webapps/12[01;31m[K21[m[K9.txt

mpg123 pre0.59s - Invalid MP3 Header Memory Corruption
| linux/remote/2[01;31m[K21[m[K47.c

MRBS 1.2.x - 'view_entry.php' SQL Injection
| php/webapps/309[01;31m[K21[m[K.txt

MTink 0.9.x - Printer Status Monitor Environment Variable Buffer
Overflow |
linux/local/2[01;31m[K21[m[K89.txt

MTPutty 1.0.1.[01;31m[K21[m[K - SSH Password Disclosure
| windows/local/50574.txt

Multiple Vendor 'librpc.dll' Signedness Error - Remote Code Execution
| multiple/dos/1[01;31m[K21[m[K09.txt

Murus 1.4.11 - Local Privilege Escalation
| macos/local/43[01;31m[K21[m[K7.sh

Music Tag Editor 1.61 build [01;31m[K21[m[K2 - Remote Buffer Overflow
(PoC) |
windows/dos/9167.txt

Musoo 0.[01;31m[K21[m[K - Remote File Inclusion
| php/webapps/4085.txt

Muviko 1.0 - 'q' SQL Injection
| php/webapps/424[01;31m[K21[m[K.txt

MV Video Sharing Software 1.2 - 'searchname' SQL Injection
| php/webapps/456[01;31m[K21[m[K.txt

MVCnPHP 3.0 - glConf[path_libraries] Remote File Inclusion
| php/webapps/[01;31m[K21[m[K73.txt

MVPower DVR TV-7104HE 1.8.4 115[01;31m[K21[m[K5B9 - Shell Command
Execution (Metasploit) |
arm/remote/41471.rb

mxBB Module mx_modsdb 1.0 - Remote File Inclusion
| php/webapps/29[01;31m[K21[m[K.txt

My Little Forum 2.3.5 - PHP Command Injection
| php/webapps/400[01;31m[K21[m[K.php

My Little Weblog 2006.11.[01;31m[K21[m[K - 'Weblog.php' Cross-Site
Scripting |
php/webapps/29162.txt

My Postcards 6.0 - 'MagicCard.cgi' Arbitrary File Disclosure
| cgi/webapps/[01;31m[K21[m[K558.txt

My School Script - Database Disclosure
| asp/webapps/1[01;31m[K21[m[K99.txt

My Web Server 1.0.1/1.0.2 - GET Denial of Service
| windows/dos/[01;31m[K21[m[K935.txt

MyAuth3 - Blind SQL Injection
| php/webapps/[01;31m[K21[m[K787.rb

MyBB 1.8.32 - Remote Code Execution (RCE) (Authenticated)
| php/webapps/51[01;31m[K21[m[K3.py

```
MyBB < 1.8.[01;31m[K21[m[K - Remote Code Execution
| php/webapps/47161.php

MyBloggie 2.1.4 - 'trackback.php' Multiple SQL Injections
| php/webapps/[01;31m[K21[m[K18.php

mygamingladder MGL Combo System 7.5 - SQL Injection
| php/webapps/1[01;31m[K21[m[K35.txt

MyGuestbook 1.0 - Script Injection
| cgi/webapps/[01;31m[K21[m[K433.txt

MyHelpDesk 20020509 - Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K526.txt

MyHelpDesk 20020509 - HTML Injection
| php/webapps/[01;31m[K21[m[K519.txt

MyHelpDesk 20020509 - SQL Injection
| php/webapps/[01;31m[K21[m[K527.txt

MyMarket 1.71 - 'Form_Header.php' Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K961.txt

myPHPNuke 1.8.8 - 'Default_Theme' Cross-Site Scripting
| php/webapps/2[01;31m[K21[m[K33.txt

MyRoom 3.5 GOLD - 'save_item.php' Arbitrary File Upload
| php/webapps/2[01;31m[K21[m[K86.txt

mySeatXT 0.1781 - SQL Injection
| php/webapps/17[01;31m[K21[m[K1.txt

mySeatXT 0.[01;31m[K21[m[K34 - SQL Injection
| php/webapps/31144.txt

MyServer 0.8.9 - Filename Parse Error Information Disclosure
| multiple/remote/30[01;31m[K21[m[K9.txt

MySimpleNews 1.0 - PHP Injection
| php/webapps/[01;31m[K21[m[K900.txt

MySimpleNews 1.0 - Remote Readable Administrator Password
| php/webapps/[01;31m[K21[m[K901.txt

MySpace Clone 2010 - SQL Injection / Cross-Site Scripting
| php/webapps/34[01;31m[K21[m[K5.txt

MySpace Resource Script (MSRS) 1.[01;31m[K21[m[K - Remote File
Inclusion                                                    |
php/webapps/4585.txt
```

MySQL 3.20.32/3.22.x/3.23.x - Null Root Password Weak Default Configuration (1) | linux/remote/[01;31m[K21[m[K725.c

MySQL 3.20.32/3.22.x/3.23.x - Null Root Password Weak Default Configuration (2) | linux/remote/[01;31m[K21[m[K726.c

MySQL 3.22.27/3.22.29/3.23.8 - GRANT Global Password Changing | multiple/local/197[01;31m[K21[m[K.txt

MySQL 4.x - CREATE FUNCTION mysql.func Table Arbitrary Library Injection | multiple/remote/25[01;31m[K21[m[K0.php

MySQL 4.x - CREATE Temporary TABLE Symlink Privilege Escalation | multiple/remote/25[01;31m[K21[m[K1.c

MySQLDumper 1.[01;31m[K21[m[K - 'sql.php' Cross-Site Scripting | php/webapps/28783.txt

MyWebServer 1.0.2 - Long HTTP Request HTML Injection | windows/remote/[01;31m[K21[m[K710.txt

MyWebServer 1.0.2 - Search Request Remote Buffer Overflow | windows/remote/[01;31m[K21[m[K709.pl

n-cms-equipe 1.1c.Debug - Multiple Local File Inclusions | php/webapps/338[01;31m[K21[m[K.html

N/X Web Content Management System 2002 Prerelease 1 - 'datasets.php?c_path' Local File Inclusion | php/webapps/2[01;31m[K21[m[K16.txt

N/X Web Content Management System 2002 Prerelease 1 - 'menu.inc.php?c_path' Remote File Inclusion | php/webapps/2[01;31m[K21[m[K15.txt

Nagios < 4.2.4 - Local Privilege Escalation | linux/local/409[01;31m[K21[m[K.sh

Nagios Log Server 2024R1.3.1 - API Key Exposure | multiple/webapps/5[01;31m[K21[m[K77.md

Nagios Log Server 2024R1.3.1 - Stored XSS | multiple/webapps/5[01;31m[K21[m[K17.md

Nagios Network Analyzer 2.2.1 - Multiple Cross-Site Request Forgery Vulnerabilities | php/webapps/402[01;31m[K21[m[K.txt

Nagios XI 5.5.6 - Remote Code Execution / Privilege Escalation | linux/webapps/462[01;31m[K21[m[K.py

```
Nagios Xi 5.6.6 - Authenticated Remote Code Execution (RCE)
| multiple/webapps/5[01;31m[K21[m[K38.txt

National Instruments LabVIEW 5.1.1/6.0/6.1 - HTTP Request Denial of
Service                                  |
multiple/dos/[01;31m[K21[m[K413.txt

Navigate CMS 2.9.4 - Server-Side Request Forgery (SSRF) (Authenticated)
| php/webapps/509[01;31m[K21[m[K.py

Navis Webaccess - SQL Injection
| jsp/webapps/40[01;31m[K21[m[K6.txt

NCMedia Sound Editor Pro 7.5.1 - 'MRUList201202.dat' File Handling
Buffer Overflow                          |
windows/local/[01;31m[K21[m[K331.py

NCMedia Sound Editor Pro 7.5.1 - Local Overflow (SEH + DEP Bypass)
| windows/local/[01;31m[K21[m[K713.py

NCSA HTTPd 1.x - Remote Buffer Overflow (1)
| linux/remote/[01;31m[K21[m[K049.c

NCSA HTTPd 1.x - Remote Buffer Overflow (2)
| linux/remote/[01;31m[K21[m[K050.c

NCSS 07.1.[01;31m[K21[m[K - Array Overflow with Write2
| windows/dos/17903.txt

NeoBill CMS 0.8 Alpha - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K317.txt

Net Monitor for Employees Pro < 5.3.4 - Unquoted Service Path Privilege
Escalation                           |
windows/local/4[01;31m[K21[m[K41.txt

Net-SNMP 4.2.3 - snmpnetstat Remote Heap Overflow
| linux/remote/[01;31m[K21[m[K200.c

NetBSD 1.x - 'TalkD' User Validation
| netbsd_x86/remote/[01;31m[K21[m[K364.txt

NetGear D1500 V1.0.0.[01;31m[K21[m[K_1.0.1PE - 'Wireless Repeater'
Stored Cross-Site Scripting (XSS)                    |
hardware/webapps/50201.txt

Netgear MA5[01;31m[K21[m[K Wireless Driver 5.148.724 - 'Beacon Probe'
Remote Buffer Overflow                               |
windows/remote/29096.rb

Netman 204 - Remote command without authentication
| multiple/hardware/5[01;31m[K21[m[K83.txt
```

```
Netopia Timbuktu Pro for Macintosh 6.0.1 - Denial of Service
| osx/dos/[01;31m[K21[m[K234.sh

Netris 0.3/0.4/0.5 - Remote Memory Corruption
| linux/remote/[01;31m[K21[m[K784.c

Netscape 4.77 - Composer Font Face Field Buffer Overflow
| multiple/dos/[01;31m[K21[m[K544.html

Netscape 4.x/6.x / Mozilla 0.9.x - Malformed Email POP3 Denial of
Service                                    |
multiple/dos/[01;31m[K21[m[K539.c

Netscape Enterprise Web Server for Netware 4/5 5.0 - Information
Disclosure                                  |
novell/remote/[01;31m[K21[m[K488.txt

Netsweeper WebAdmin Portal - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K330.txt

NetWin DMail 2.x / SurgeFTP 1.0/2.0 - Weak Password Encryption
| multiple/local/[01;31m[K21[m[K020.c

Network Shutdown Module 3.[01;31m[K21[m[K - 'sort_values' Remote PHP
Code Injection (Metasploit)                        |
php/remote/23006.rb

NewAtlanta ServletExec/ISAPI 4.1 - File Disclosure
| windows/remote/[01;31m[K21[m[K470.txt

NewAtlanta ServletExec/ISAPI 4.1 - Full Path Disclosure
| windows/remote/[01;31m[K21[m[K469.txt

NewAtlanta ServletExec/ISAPI 4.1 JSPServlet - Denial of Service
| windows/dos/[01;31m[K21[m[K471.c

NEWS-BUZZ News Management System 1.0 - SQL Injection
| php/webapps/5[01;31m[K21[m[K74.txt

NEWSolved Lite 1.9.2 - 'abs_path' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K35.txt

newsPHP [01;31m[K21[m[K6 - Authentication Bypass
| php/webapps/23058.txt

newsPHP [01;31m[K21[m[K6 - Remote File Inclusion
| php/webapps/23057.txt

newsReporter 1.1 - 'index.php' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K01.txt

Next.js Middleware 15.2.2 -  Authorization Bypass
| multiple/webapps/5[01;31m[K21[m[K24.txt
```

Nintendo Switch - WebKit Code Execution (PoC)
| hardware/dos/44[01;31m[K21[m[K3.html

Nitrotech 0.0.3a - Remote File Inclusion / SQL Injection
| php/webapps/7[01;31m[K21[m[K8.txt

Noahs Classifieds 1.3 - 'lowerTemplate' Remote Code Execution
| php/webapps/15[01;31m[K21[m[K.php

NOCC 0.9.x - Webmail Script Injection
| php/webapps/[01;31m[K21[m[K449.txt

Nokia Symbian 60 3rd Edition - Browser Crash (Denial of Service)
| hardware/dos/[01;31m[K21[m[K76.html

Nortel CVX 1800 Multi-Service Access Switch - Default SNMP Community
| hardware/remote/[01;31m[K21[m[K378.txt

Northern Solutions Xeneo Web Server 2.1/2.2 - Denial of Service
| windows/dos/[01;31m[K21[m[K982.txt

Noticeware Email Server 4.6 - NG LOGIN Messages Denial of Service
| multiple/dos/3[01;31m[K21[m[K94.txt

Novell Groupwise 5.5/6.0 Servlet Gateway - Default Authentication
| novell/remote/[01;31m[K21[m[K182.txt

Novell Groupwise 8.0.2 HP3 and 2012 - Integer Overflow
| windows/dos/[01;31m[K21[m[K326.txt

Novell Groupwise Client 7.0.3.1294 - 'gxmim1.dll' ActiveX Control
Buffer Overflow (PoC) |
windows/dos/332[01;31m[K21[m[K.html

Novell NetWare 5.1/6.0 - POST Arbitrary Perl Code Execution
| novell/remote/[01;31m[K21[m[K731.pl

novell sentinel log manager 1.2.0.1 - Directory Traversal
| multiple/webapps/[01;31m[K21[m[K082.txt

Novell Sentinel Log Manager 1.2.0.2 - Retention Policy
| windows/webapps/[01;31m[K21[m[K744.txt

Novell ZENworks Configuration Management Preboot Service
0x[01;31m[K21[m[K - Remote Buffer Overflow (Metasploit) |
windows/remote/19932.rb

Novus 1.0 - 'Buscar.asp' Cross-Site Scripting
| asp/webapps/306[01;31m[K21[m[K.txt

NPDS 4.8 - News Message HTML Injection
| php/webapps/[01;31m[K21[m[K860.txt

```
NSI Rwhoisd 1.5 - Remote Format String
| unix/remote/[01;31m[K21[m[K128.c

ntop-ng 2.0.1510[01;31m[K21[m[K - Privilege Escalation
| multiple/webapps/38836.txt

NTR - ActiveX Control 'Check()' Method Buffer Overflow (Metasploit)
| windows/remote/[01;31m[K21[m[K841.rb

NTR - ActiveX Control 'StopModule()' Remote Code Execution (Metasploit)
| windows/remote/[01;31m[K21[m[K839.rb

nuevoMailer 6.0 - SQL Injection
| php/webapps/4[01;31m[K21[m[K93.txt

Nuevomailer < 6.0 - SQL Injection
| php/webapps/4[01;31m[K21[m[K64.txt

Nuked-klaN 1.7.7 - Remote File Inclusion
| php/webapps/107[01;31m[K21[m[K.txt

NukeHall 0.3 - Multiple Remote File Inclusions
| php/webapps/10[01;31m[K21[m[K7.txt

Null HTTPd 0.5 - Remote Heap Overflow
| linux/remote/[01;31m[K21[m[K818.c

NullLogic Null HTTPd 0.5 - Error Page Cross-Site Scripting
| multiple/remote/[01;31m[K21[m[K767.txt

Nullsoft SHOUTcast 1.8.9 - Remote Buffer Overflow
| multiple/remote/[01;31m[K21[m[K511.c

Nullsoft Winamp 2.80 - Automatic Update Check Buffer Overflow
| windows/remote/[01;31m[K21[m[K595.c

NUUO NVRmini 2 3.0.8 - 'strong_user.php' Backdoor Remote Shell Access
| php/webapps/40[01;31m[K21[m[K5.txt

NUUO NVRmini 2 3.0.8 - Arbitrary File Deletion
| php/webapps/40[01;31m[K21[m[K4.txt

NUUO NVRmini 2 3.0.8 - Cross-Site Request Forgery (Add Admin)
| php/webapps/40[01;31m[K21[m[K0.html

NUUO NVRmini 2 3.0.8 - Local File Disclosure
| php/webapps/40[01;31m[K21[m[K1.txt

NUUO NVRmini 2 3.0.8 - Multiple OS Command Injections
| php/webapps/40[01;31m[K21[m[K2.txt

NUUO NVRmini 2 3.0.8 - Remote Command Injection (Shellshock)
| cgi/webapps/40[01;31m[K21[m[K3.txt
```

NVIDIA Update Service Daemon 1.0.[01;31m[K21[m[K - 'nvUpdatusService' Unquoted Service Path | windows/local/48391.txt

Nxlog Community Edition 2.10.[01;31m[K21[m[K50 - DoS (Poc) | multiple/dos/49283.txt

OCE 31[01;31m[K21[m[K/3122 Printer - 'parser.exe' Denial of Service | hardware/dos/1718.pl

Oddsock Song Requester 2.1 WinAmp Plugin - Denial of Service | cgi/dos/[01;31m[K21[m[K620.txt

ollama 0.6.4 - Server Side Request Forgery (SSRF) | multiple/local/5[01;31m[K21[m[K16.py

OmniHTTPd 1.1/2.0.x/2.4 - 'test.php' Sample Application Cross-Site Scripting | windows/remote/[01;31m[K21[m[K753.txt

OmniHTTPd 1.1/2.0.x/2.4 - Sample Application URL Encoded Newline HTML Injection | windows/remote/[01;31m[K21[m[K757.txt

OmniHTTPd 1.1/2.0.x/2.4 - test.shtml Sample Application Cross-Site Scripting | windows/remote/[01;31m[K21[m[K754.txt

Omnistar Document Manager 8.0 - Multiple Vulnerabilities | php/webapps/[01;31m[K21[m[K890.txt

Omnistar Mailer 7.2 - Multiple Vulnerabilities | php/webapps/[01;31m[K21[m[K716.txt

OneCMS 2.6.1 - 'cat' Cross-Site Scripting | php/webapps/34[01;31m[K21[m[K0.txt

OneCMS 2.6.1 - 'search' SQL Injection | php/webapps/34[01;31m[K21[m[K1.html

OneCMS 2.6.1 - 'short1' Cross-Site Scripting | php/webapps/34[01;31m[K21[m[K2.html

OnePC mySite Management Software - SQL Injection | php/webapps/1[01;31m[K21[m[K57.txt

Online Bus Ticket Reservation 1.0 - SQL Injection | php/webapps/49[01;31m[K21[m[K2.txt

Online Movie Streaming 1.0 - Admin Authentication Bypass | php/webapps/494[01;31m[K21[m[K.txt

```
Online Thesis Archiving System v1.0 - Multiple-SQLi
| php/webapps/515[01;31m[K21[m[K.txt

Online Traffic Offense Management System 1.0 - 'id' SQL Injection
(Authenticated)                              |
php/webapps/50[01;31m[K21[m[K8.txt

Online Traffic Offense Management System 1.0 - Remote Code Execution
(RCE) (Unauthenticated)                |
php/webapps/502[01;31m[K21[m[K.py

OPAC EasyWeb Five 5.7 - 'nome' SQL Injection
| php/webapps/455[01;31m[K21[m[K.txt

Open Flash Chart 2 - Arbitrary File Upload (Metasploit)
| php/remote/29[01;31m[K21[m[K0.rb

Open-School 3.0 / Community Edition 2.3 - Cross-Site Scripting
| php/webapps/47[01;31m[K21[m[K2.txt

OpenBB 1.0 - Unauthorized Moderator Access
| php/webapps/[01;31m[K21[m[K478.txt

OpenBB 1.0.0 RC3 - BBCode Cross Agent HTML Injection
| php/webapps/[01;31m[K21[m[K474.txt

OpenBB 1.0.0 RC3 - Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K479.txt

OpenBB 1.0.x - Image Tag Cross-Agent Scripting
| php/webapps/[01;31m[K21[m[K301.txt

OpenBSD 2.9/3.0 - Default Crontab Root Command Injection
| openbsd/local/[01;31m[K21[m[K373.c

OpenBSD 2.x/3.0 - User Mode Return Value Denial of Service
| openbsd/dos/[01;31m[K21[m[K167.c

OpenBSD 2.x/3.x - CHPass Temporary File Link File Content Revealing
| openbsd/local/22[01;31m[K21[m[K0.txt

OpenCart - Cross-Site Request Forgery (Change User Password)
| php/webapps/249[01;31m[K21[m[K.txt

Opencart 3.0.3.2 - 'extension/feed/google_base' Denial of Service (PoC)
| php/dos/469[01;31m[K21[m[K.sh

OpenFAQ 0.4 - 'Validate.php' HTML Injection
| php/webapps/278[01;31m[K21[m[K.html

OpenFiler 2.x - NetworkCard Command Execution (Metasploit)
| linux/remote/[01;31m[K21[m[K191.rb
```

OpenMPT 1.17.02.43 - Multiple Remote Buffer Overflows (PoC)
| windows/dos/[01;31m[K21[m[K60.c

OpenPanel 0.3.4 - Directory Traversal
| multiple/webapps/5[01;31m[K21[m[K95.txt

OpenPanel 0.3.4 - Incorrect Access Control
| multiple/webapps/5[01;31m[K21[m[K96.txt

OpenPanel 0.3.4 - OS Command Injection
| multiple/webapps/5[01;31m[K21[m[K97.txt

OpenPanel Copy and View functions in the File Manager 0.3.4 - Directory Traversal |
multiple/webapps/5[01;31m[K21[m[K98.txt

OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
| linux/remote/45[01;31m[K21[m[K0.py

OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by-One
| unix/remote/[01;31m[K21[m[K314.txt

OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow
| linux/remote/[01;31m[K21[m[K402.txt

OpenSSH 3.x - Challenge-Response Buffer Overflow (1)
| unix/remote/[01;31m[K21[m[K578.txt

OpenSSH 3.x - Challenge-Response Buffer Overflow (2)
| unix/remote/[01;31m[K21[m[K579.txt

Opentel Openmairie tel 1.02 - Local File Inclusion
| php/webapps/12[01;31m[K21[m[K2.txt

OpenTopic 2.3.1 - Private Message HTML Injection
| php/webapps/2[01;31m[K21[m[K25.txt

Openurgence vaccin 1.03 - Local File Inclusion / Remote File Inclusion
| php/webapps/1[01;31m[K21[m[K93.txt

OpenVms 5.3/6.2/7.x - UCX POP Server Arbitrary File Modification
| multiple/local/[01;31m[K21[m[K856.txt

OpenVms 8.3 Finger Service - Stack Buffer Overflow
| multiple/dos/3[01;31m[K21[m[K93.txt

Opera 5.0/5.1 - Same Origin Policy Circumvention
| windows/remote/[01;31m[K21[m[K156.txt

Opera 5.12/6.0 - Frame Location Same Origin Policy Circumvention
| windows/remote/[01;31m[K21[m[K451.txt

```
Opera 6.0.1 / Microsoft Internet Explorer 5/6 - JavaScript Modifier
Keypress Event Subversion              |
windows/remote/[01;31m[K21[m[K636.txt

Opera 6.0.1/6.0.2 - Arbitrary File Disclosure
| windows/remote/[01;31m[K21[m[K483.html

Opera 6.0.x - FTP View Cross-Site Scripting
| windows/remote/[01;31m[K21[m[K681.html

Opera 7 - Image Rendering HTML Injection
| windows/remote/22[01;31m[K21[m[K7.txt

Opera 7.0 - Error Message History Disclosure
| windows/remote/22[01;31m[K21[m[K9.txt

Opera 7.0 - History Object Information Disclosure
| windows/remote/22[01;31m[K21[m[K8.txt

Opera 7.0 - JavaScript Console Attribute Injection
| windows/remote/22[01;31m[K21[m[K3.txt

Opera 9 - IRC Client Remote Denial of Service
| multiple/dos/[01;31m[K21[m[K79.c

Opera 9 IRC Client - Remote Denial of Service
| multiple/dos/[01;31m[K21[m[K80.py

OPT Max 1.2.0 - 'CRM_inc' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K92.txt

Oracle 8.1.x/9.0/9.2 - TNS Listener Service_CurLoad Remote Denial of
Service                                |
multiple/dos/[01;31m[K21[m[K782.txt

Oracle 8/9i - DBSNMP Oracle Home Environment Variable Buffer Overflow
| windows/local/[01;31m[K21[m[K044.c

Oracle 8i - 'dbsnmp' Remote Denial of Service
| multiple/dos/[01;31m[K21[m[K232.c

Oracle 8i - TNS Listener Local Command Parameter Buffer Overflow
| linux/local/[01;31m[K21[m[K362.c

Oracle 9i Application Server 9.0.2 Web Cache Administration Tool -
Denial of Service                       |
multiple/dos/[01;31m[K21[m[K911.txt

Oracle Business Transaction Management FlashTunnelService - Remote Code
Execution (Metasploit)             | java/remote/[01;31m[K21[m[K846.rb

Oracle MySQL < 5.1.49 - Malformed 'BINLOG' Arguments Denial of Service
| linux/dos/345[01;31m[K21[m[K.txt
```

Oracle OTRCREP Oracle 8/9 - Home Environment Variable Buffer Overflow
| unix/local/[01;31m[K21[m[K045.c

Oracle Reports Server 6.0.8/9.0.2 - Information Disclosure
| multiple/remote/[01;31m[K21[m[K627.txt

Oracle VirtualBox Manager 5.2.18 r124319 - 'Name Attribute' Denial of Service (PoC) | windows_x86-64/dos/454[01;31m[K21[m[K.py

Oracle VM VirtualBox 4.1 - Local Denial of Service
| linux_x86-64/dos/[01;31m[K21[m[K224.c

Oracle9iAS Web Cache 2.0 - Remote Buffer Overflow
| windows/remote/[01;31m[K21[m[K1[01;31m[K21[m[K.pl

OrangeHRM 2.6.3 - 'PluginController.php' Local File Inclusion
| php/webapps/17[01;31m[K21[m[K2.txt

Orinoco OEM Residential Gateway - SNMP Community String Remote Configuration | hardware/remote/[01;31m[K21[m[K699.txt

OS/400 - User Account Name Disclosure
| multiple/local/[01;31m[K21[m[K283.txt

osCommerce 2.1 - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K563.txt

osCSS 2.1 - Multiple Cross-Site Scripting / Local File Inclusions
| php/webapps/355[01;31m[K21[m[K.txt

osData 2.08 Modules Php1[01;31m[K21[m[K - Local File Inclusion
| php/webapps/4870.txt

Osprey 1.0a4.1 - 'ListRecords.php' Multiple Remote File Inclusions
| php/webapps/325[01;31m[K21[m[K.txt

Outfront Spooky 2.x - Login SQL Query Manipulation Password
| asp/webapps/[01;31m[K21[m[K434.txt

Outlook Express 6 - Attachment Security Bypass
| windows/local/[01;31m[K21[m[K096.txt

Outpost Security Suite Pro 2009 - Filename Parsing Security Bypass
| multiple/remote/3[01;31m[K21[m[K10.txt

outreach project tool 1.2.6 - Remote File Inclusion
| php/webapps/10[01;31m[K21[m[K8.txt

Owl Intranet Engine 0.95 - 'register.php' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K22.txt

ownCloud 4.0.x/4.5.x - 'upload.php?Filename' Remote Code Execution
| multiple/webapps/3[01;31m[K21[m[K62.txt

oXygen XML Editor [01;31m[K21[m[K.1.1 - XML External Entity Injection
| windows/local/47658.txt

p.mapper 3.2 beta3 - '/plugins/export/mc_table.php?_SESSION[PM_INCPHP]'
Remote File Inclusion | php/webapps/308[01;31m[K21[m[K.txt

Pablo Software Solutions FTP Service 1.2 - Anonymous Users Privileges
| windows/remote/227[01;31m[K21[m[K.txt

PAFileDB 1.1.3/2.1.1/3.0/3.1 - 'category.php?start' Cross-Site
Scripting |
php/webapps/25[01;31m[K21[m[K6.txt

PAFileDB 1.1.3/2.1.1/3.0/3.1 - 'category.php?start' SQL Injection
| php/webapps/25[01;31m[K21[m[K4.txt

PAFileDB 1.1.3/2.1.1/3.0/3.1 - 'viewall.php?start' Cross-Site Scripting
| php/webapps/25[01;31m[K21[m[K5.txt

PAFileDB 1.1.3/2.1.1/3.0/3.1 - 'viewall.php?start' SQL Injection
| php/webapps/25[01;31m[K21[m[K3.txt

Palo Alto Networks Expedition 1.2.90.1 - Admin Account Takeover
| multiple/webapps/5[01;31m[K21[m[K29.py

PandoraFMS 7.0NG.772 - SQL Injection
| php/webapps/5[01;31m[K21[m[K57.py

Parallels Desktop - Virtual Machine Escape
| windows/local/4[01;31m[K21[m[K16.txt

Password Manager Pro / Pro MSP - Blind SQL Injection
| multiple/webapps/35[01;31m[K21[m[K0.txt

patBBcode 1.0 - 'bbcodeSource.php' Remote File Inclusion
| php/webapps/46[01;31m[K21[m[K.txt

PaulShop - SQL Injection
| php/webapps/4[01;31m[K21[m[K56.txt

Payara Micro Community 5.20[01;31m[K21[m[K.6 - Directory Traversal
| multiple/webapps/50371.txt

pbboard 2.1.1 - Multiple Vulnerabilities
| php/webapps/151[01;31m[K21[m[K.txt

Pcshey Portal - 'kategori.asp' SQL Injection
| asp/webapps/3[01;31m[K21[m[K51.pl

pdfium - opj_jp2_apply_pclr 'libopenjpeg' Heap Out-of-Bounds Read
| multiple/dos/393[01;31m[K21[m[K.txt

PEEL 1.0b - Remote File Inclusion
| php/webapps/2[01;31m[K21[m[K14.txt

PeerCast 0.1[01;31m[K21[m[K1 - Remote Format String
| linux/remote/1055.c

PeerCast 0.1[01;31m[K21[m[K6 (Linux) - URL Handling Buffer Overflow
(Metasploit) |
linux/remote/16855.rb

PeerCast 0.1[01;31m[K21[m[K6 (Windows x86) - URL Handling Buffer
Overflow (Metasploit) |
windows_x86/remote/16786.rb

PeerCast 0.1[01;31m[K21[m[K6 - 'nextCGIarg' Remote Buffer Overflow (1)
| linux/remote/1574.c

PeerCast 0.1[01;31m[K21[m[K6 - 'nextCGIarg' Remote Buffer Overflow (2)
| linux/remote/1578.c

PeerCast 0.1[01;31m[K21[m[K6 - Remote Buffer Overflow (Metasploit)
| windows/remote/1626.pm

PeerCast 0.1[01;31m[K21[m[K6 - Remote Stack Overflow (Metasploit)
| linux/remote/10027.rb

PeerCast 0.1[01;31m[K21[m[K8 - 'getAuthUserPass' Multiple Buffer
Overflow Vulnerabilities |
linux/dos/31713.py

Peercast < 0.1[01;31m[K21[m[K1 - Format
String
| windows/dos/43826.txt

Pegasus Mail 4.0 1 - Message Header Buffer Overflow
| windows/remote/[01;31m[K21[m[K648.txt

Peplink Balance Routers 7.0.0-build1904 - SQL Injection / Cross-Site
Scripting / Information Disclosure |
cgi/webapps/4[01;31m[K21[m[K30.txt

Perception LiteServe 2.0.1 - Directory Query String Cross-Site
Scripting |
windows/remote/[01;31m[K21[m[K999.txt

Perception LiteServe 2.0.1 - DNS Wildcard Cross-Site Scripting
| windows/remote/[01;31m[K21[m[K997.txt

Perch v3.2 - Stored XSS
| php/webapps/516[01;31m[K21[m[K.txt

Perspective ICM Investigation & Case 5.1.1.16 - Privilege Escalation
| windows/webapps/43[01;31m[K21[m[K0.txt

PgMarket 2.2.3 - 'CFG[libdir]' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K54.txt

PHF (Linux/x86) - Remote Buffer Overflow
| cgi/remote/[01;31m[K21[m[K1.c

Philip Chinery's Guestbook 1.1 - Script Injection
| cgi/webapps/[01;31m[K21[m[K406.txt

PHlyMail Lite 3.4.4 - 'mod.listmail.php' Remote File Inclusion
| php/webapps/2[01;31m[K21[m[K1.txt

phNNTP 1.3 - 'article-raw.php' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K48.txt

Phorum 3.3.2 - Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K461.txt

Phorum 3.3.2a - Remote Command Execution
| php/webapps/[01;31m[K21[m[K459.txt

Photo Video Album Transfer 1.0 iOS - Multiple Vulnerabilities
| ios/webapps/30[01;31m[K21[m[K5.txt

PhotoCycle 1.0 - 'PhotoCycle.php' Cross-Site Scripting
| php/webapps/28[01;31m[K21[m[K4.txt

Photodex ProShow Producer 5.0.3310 - Local Buffer Overflow (SEH)
| windows/local/29[01;31m[K21[m[K3.pl

PHP 3.0.x/4.x - Move_Uploaded_File open_basedir Circumvention
| php/local/[01;31m[K21[m[K347.php

PHP 4.2.3 - Header Function Script Injection
| php/webapps/[01;31m[K21[m[K776.txt

PHP 4.4.3/5.1.4 - 'objIndex' Local Buffer Overflow
| php/local/[01;31m[K21[m[K52.php

PHP 4.4.3/5.1.4 - 'sscanf' Local Buffer Overflow
| linux/local/[01;31m[K21[m[K93.php

PHP 4.x/5.x MySQL Library - 'Safe_mode' Filesystem Circumvention (1)
| php/remote/[01;31m[K21[m[K264.php

PHP 4.x/5.x MySQL Library - 'Safe_mode' Filesystem Circumvention (2)
| php/remote/[01;31m[K21[m[K265.php

PHP 4.x/5.x MySQL Library - 'Safe_mode' Filesystem Circumvention (3)
| php/remote/[01;31m[K21[m[K266.php

```
PHP 5.2.3 Win32std - 'win_shell_execute' Safe Mode / disable_functions
Bypass                                  |
windows/local/4[01;31m[K21[m[K8.php

PHP 5.3.0 - 'getopt()' Denial of Service
| multiple/dos/1[01;31m[K21[m[K65.txt

PHP 5.3.4 Win Com Module - Com_sink
| windows/local/[01;31m[K21[m[K887.php

PHP 6.0 Dev - 'str_transliterate()' Local Buffer Overflow (NX + ASLR
Bypass)                                   |
windows/local/1[01;31m[K21[m[K89.php

PHP 7.0 - 'AppendIterator::append' Local Denial of Service
| php/dos/403[01;31m[K21[m[K.php

PHP Address Book 7.0 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/37[01;31m[K21[m[K9.txt

PHP Advanced Transfer Manager 1.[01;31m[K21[m[K - Arbitrary File
Inclusion                                                 |
php/webapps/25686.txt

PHP Advanced Transfer Manager 1.[01;31m[K21[m[K - Arbitrary File Upload
| php/remote/25627.txt

PHP Arena PAFileDB 1.1.3/2.1.1/3.0 - 'Email To Friend' Cross-Site
Scripting                                    |
php/webapps/[01;31m[K21[m[K957.txt

PHP Bible Search - 'bible.php?chapter' Cross-Site Scripting
| php/webapps/34[01;31m[K21[m[K4.txt

PHP Bible Search - 'bible.php?chapter' SQL Injection
| php/webapps/34[01;31m[K21[m[K3.txt

PHP City Portal Script Software - SQL Injection
| php/webapps/18[01;31m[K21[m[K0.txt

PHP Classifieds 6.0.5 - Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K552.txt

PHP Dashboards NEW 5.8 - 'dashID' SQL Injection
| php/webapps/46[01;31m[K21[m[K2.txt

PHP Dashboards NEW 5.8 - Local File Inclusion
| php/webapps/46[01;31m[K21[m[K3.txt

PHP Director 0.[01;31m[K21[m[K - Remote Command Execution
| php/webapps/8014.pl
```

```
PHP Director 0.[01;31m[K21[m[K - SQL Into Outfile 'eval()' Injection
| php/webapps/8181.c

PHP Event Calendar 1.4 - 'calendar.php' Remote File Inclusion
| php/webapps/28[01;31m[K21[m[K5.txt

PHP Generic library & Framework - 'INCLUDE_PATH' Remote File Inclusion
| php/webapps/3[01;31m[K21[m[K7.txt

PHP GMP - 'unserialize()' Use-After-Free
| php/dos/381[01;31m[K21[m[K.txt

PHP iCalendar 2.[01;31m[K21[m[K - 'cookie' Remote Code Execution
| php/webapps/1585.php

PHP iCalendar 2.[01;31m[K21[m[K - 'publish.ical.php' Remote Code
Execution                                                 |
php/webapps/1586.php

PHP Interpreter 3.0.x/4.0.x/4.1/4.2 - Direct Invocation Denial of
Service                                  |
unix/dos/[01;31m[K21[m[K632.c

PHP JackKnife 2.[01;31m[K21[m[K - '(PHPJK) G_Display.php' Multiple
Cross-Site Scripting Vulnerabilities                |
php/webapps/30116.txt

PHP JackKnife 2.[01;31m[K21[m[K - '(PHPJK) G_Display.php?iCategoryUnq'
SQL Injection                                       |
php/webapps/30112.txt

PHP JackKnife 2.[01;31m[K21[m[K - '/(PHPJK)
Search/DisplayResults.php?iSearchID' SQL Injection
| php/webapps/30113.txt

PHP JackKnife 2.[01;31m[K21[m[K - '/(PHPJK)
UserArea/Authenticate.php?sUName' Cross-Site Scripting
| php/webapps/30114.txt

PHP JackKnife 2.[01;31m[K21[m[K - '/(PHPJK)
UserArea/NewAccounts/index.php?sAccountUnq' Cross-Site Scripting
| php/webapps/30115.txt

PHP JackKnife 2.[01;31m[K21[m[K - Cross-Site Scripting
| php/webapps/26797.txt

PHP Links 1.3 - 'id' SQL Injection
| php/webapps/50[01;31m[K21[m[K.txt

PHP Live Helper 2.0 - 'abs_path' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K20.txt
```

```
PHP Quick Arcade 3.0.[01;31m[K21[m[K - Multiple Vulnerabilities
| php/webapps/12416.txt

PHP Simple Shop 2.0 - 'abs_path' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K19.txt

PHP TopSites 2.0/2.2 - 'edit.php' SQL Injection
| php/webapps/2[01;31m[K21[m[K77.txt

PHP TopSites 2.0/2.2 - 'help.php' Cross-Site Scripting
| php/webapps/2[01;31m[K21[m[K76.txt

PHP TopSites 2.0/2.2 - HTML Injection
| php/webapps/2[01;31m[K21[m[K75.txt

PHP Uber-style GeoTracking 1.1 - SQL Injection
| php/webapps/46[01;31m[K21[m[K4.txt

PHP-Address 0.2 e - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K564.txt

PHP-Nuke 1.0/2.5/3.0/4.x/5.x/6.x/7.x - 'modules.php' Multiple Cross-
Site Scripting Vulnerabilities         |
php/webapps/[01;31m[K21[m[K166.txt

PHP-Nuke 1.0/2.5/3.0/4.x/5.x/6.x/7.x - 'user.php?uname' Cross-Site
Scripting                               |
php/webapps/[01;31m[K21[m[K165.txt

PHP-Nuke 4.x/5.x - Arbitrary File Inclusion
| php/webapps/[01;31m[K21[m[K230.txt

PHP-Nuke 4.x/5.x - SQL_Debug Information Disclosure
| php/webapps/[01;31m[K21[m[K233.txt

PHP-Nuke 5.0 - 'user.php' Form Element Substitution
| php/webapps/[01;31m[K21[m[K038.txt

PHP-Nuke 5.6 - 'modules.php' SQL Injection
| php/webapps/[01;31m[K21[m[K977.txt

PHP-Nuke 5.x - Error Message Web Root Disclosure
| php/webapps/[01;31m[K21[m[K349.txt

PHP-Nuke 5.x/6.0 - Avatar HTML Injection
| php/webapps/22[01;31m[K21[m[K1.txt

PHP-Nuke 6.0 - 'modules.php' Denial of Service
| php/dos/2[01;31m[K21[m[K10.txt

PHP-Nuke 6.0 - 'modules.php' SQL Injection
| php/webapps/[01;31m[K21[m[K862.txt
```

PHP-Nuke 6.0 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/2[01;31m[K21[m[K03.txt

PHP-Nuke 6.0 - Multiple Full Path Disclosure Vulnerabilities
| php/webapps/2[01;31m[K21[m[K02.txt

PHP-Nuke 6.0 - News Message HTML Injection
| php/webapps/[01;31m[K21[m[K859.txt

PHP-Nuke 6.0/6.5 - Search Form Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K855.txt

PHP-Nuke 6.x < 7.6 Top module - SQL Injection
| php/webapps/9[01;31m[K21[m[K.sh

PHP-Nuke 7.8 - 'modules.php' SQL Injection
| php/webapps/1[01;31m[K21[m[K9.c

PHP-Nuke 8.0 Downloads Module - 'query' Cross-Site Scripting
| php/webapps/330[01;31m[K21[m[K.txt

PHP-Nuke AddOn PHPToNuke.php 1.0 - Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K206.txt

PHP-Nuke Book Catalog Module 1.0 - 'catid' SQL Injection
| php/webapps/3[01;31m[K21[m[K40.txt

PHP-Nuke Kleinanzeigen Module - 'lid' SQL Injection
| php/webapps/3[01;31m[K21[m[K91.txt

PHP-Nuke Network Tool 0.2 Addon - MetaCharacter Filtering Command
Execution |
php/remote/[01;31m[K21[m[K155.txt

PHP-Wiki 1.2/1.3 - Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K622.txt

PHP1[01;31m[K21[m[K Instant Messenger 1.4 - Remote Code Execution
| php/webapps/1666.php

PHP1[01;31m[K21[m[K Instant Messenger 2.2 - Local File Inclusion
| php/webapps/3694.txt

PHPAccounts 0.5 - 'index.php' Multiple SQL Injections
| php/webapps/302[01;31m[K21[m[K.txt

PHPads [01;31m[K21[m[K3607 - Authentication Bypass / Password Change
| php/webapps/35535.php

PHPAlumni - SQL Injection
| php/webapps/76[01;31m[K21[m[K.txt

```
phpAtm 1.[01;31m[K21[m[K - 'include_location' Remote File Inclusion
| php/webapps/2279.txt

phpAuction 1/2 - Unauthorized Administrative Access
| php/webapps/[01;31m[K21[m[K590.txt

phpAuction 2.1 - 'phpAds_path' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K00.txt

phpAutoMembersArea 3.2.5 - 'installed_config_file' Remote File
Inclusion                                       |
php/webapps/[01;31m[K21[m[K32.txt

phpAutoVideo 2.[01;31m[K21[m[K - 'index.php?cat' Cross-Site Scripting
| php/webapps/31038.txt

phpAutoVideo 2.[01;31m[K21[m[K - 'sidebar.php?loadpage' Remote File
Inclusion                                                 |
php/webapps/31037.txt

PHPay 2.02 - 'nu_mail.inc.php?mail()' Remote Injection
| php/webapps/[01;31m[K21[m[K81.pl

phpBB 1.4 - SQL Query Manipulation
| php/webapps/[01;31m[K21[m[K046.txt

phpBB 1.x - Page Header Arbitrary Command Execution
| php/webapps/[01;31m[K21[m[K065.pl

phpBB 1.x/2.0.x - 'search.php?search_results' SQL Injection
| php/webapps/238[01;31m[K21[m[K.php

phpBB 2.0.[01;31m[K21[m[K - 'privmsg.php' HTML Injection
| php/webapps/29442.html

phpBB 2.0.[01;31m[K21[m[K - Poison Null Byte Remote File Upload
| php/webapps/2348.pl

phpBB 2.0.3 - 'privmsg.php' SQL Injection
| php/webapps/2[01;31m[K21[m[K82.pl

phpBB Minerva Mod 2.0.[01;31m[K21[m[K build 238a - SQL Injection
| php/webapps/3519.txt

phpBB MyPage Plugin - SQL Injection
| php/webapps/18[01;31m[K21[m[K2.txt

PHPBB2 - Image Tag HTML Injection
| php/webapps/[01;31m[K21[m[K486.txt

phpBB2 Gender Mod 1.1.3 - SQL Injection
| php/webapps/[01;31m[K21[m[K660.txt
```

PHPBBMod 1.3.3 - PHPInfo Information Disclosure
| php/webapps/[01;31m[K21[m[K931.txt

phpCC 4.2 Beta - 'base_dir' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K34.txt

PHPCodeCabinet 0.5 - 'Core.php' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K39.txt

phpCodeGenie 3.0.2 - 'BEAUT_PATH' Remote File Inclusion
| php/webapps/2[01;31m[K21[m[K2.txt

PHPCollab CMS 2.5 - 'emailusers.php' SQL Injection
| php/webapps/40[01;31m[K21[m[K8.txt

PHPDirector 0.[01;31m[K21[m[K - 'videos.php?id' SQL Injection
| php/webapps/4139.txt

PHPFreeChat 1.1 - 'demo[01;31m[K21[m[K_with_hardocded_urls.php' Cross-
Site Scripting |
php/webapps/32085.txt

PHPFreeForum 1.0 rc2 - 'error.php?message' Cross-Site Scripting
| php/webapps/318[01;31m[K21[m[K.txt

phpGB 1.1 - HTML Injection
| php/webapps/[01;31m[K21[m[K780.txt

PHPGB 1.1/1.2 - PHP Code Injection
| php/webapps/[01;31m[K21[m[K783.txt

phpGB 1.x - SQL Injection
| php/webapps/[01;31m[K21[m[K778.txt

PHPGedView 2.5/2.6 - 'Gedrecord.php' Cross-Site Scripting
| php/webapps/248[01;31m[K21[m[K.txt

phpGroupWare 0.9.13 - Debian Package Configuration
| linux/remote/[01;31m[K21[m[K365.txt

phpHeaven phpMyChat 0.14.5 - 'admin.php3' Arbitrary File Access
| php/webapps/24[01;31m[K21[m[K7.txt

phpHeaven phpMyChat 0.14.5 - 'edituser.php3?do_not_login'
Authentication Bypass |
php/webapps/24[01;31m[K21[m[K6.html

phpHeaven phpMyChat 0.14.5 - 'usersL.php3' Multiple SQL Injections
| php/webapps/24[01;31m[K21[m[K5.txt

phpIPAM 1.6 - Reflected Cross Site Scripting (XSS)
| php/webapps/5[01;31m[K21[m[K76.txt

```
PHPKB Multi-Language 9 - 'image-upload.php' Authenticated Remote Code
Execution                              |
php/webapps/482[01;31m[K21[m[K.py

PHPKB Multi-Language 9 - Authenticated Remote Code Execution
| php/webapps/48[01;31m[K21[m[K9.py

PHPKF-Portal 1.10 - 'anket_yonetim.php?portal_ayarlarportal_dili'
Traversal Local File Inclusion           |
php/webapps/3[01;31m[K21[m[K83.txt

PHPKF-Portal 1.10 - 'baslik.php?tema_dizin' Traversal Local File
Inclusion                                 |
php/webapps/3[01;31m[K21[m[K82.txt

phpLDAPadmin 0.9.6/0.9.7 - 'welcome.php' Arbitrary File Inclusion
| php/webapps/26[01;31m[K21[m[K1.txt

phpLDAPadmin 0.9.8 - 'search.php' Cross-Site Scripting
| php/webapps/277[01;31m[K21[m[K.txt

phpLDAPadmin 1.2.1.1 - Remote PHP Code Injection (1)
| php/webapps/180[01;31m[K21[m[K.php

PHPLib Team PHPLIB 7.2 - Remote Script Execution
| php/webapps/[01;31m[K21[m[K022.txt

phpLinkat 0.1 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K21[m[K906.txt

PHPLinks 2.1.2 - Add Site HTML Injection
| php/webapps/2[01;31m[K21[m[K80.txt

PHPMailer < 5.2.20 with Exim MTA - Remote Code Execution
| php/webapps/422[01;31m[K21[m[K.py

PHPMailer < 5.2.[01;31m[K21[m[K - Local File Disclosure
| php/webapps/43056.py

phpMyAdmin - '/scripts/setup.php' PHP Code Injection
| php/webapps/89[01;31m[K21[m[K.sh

phpMyAdmin 3.5.2.2 - 'server_sync.php' Backdoor (Metasploit)
| php/webapps/[01;31m[K21[m[K834.rb

phpMyBitTorrent 2.04 - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K743.txt

phpmychat plus 1.93 - Multiple Vulnerabilities
| php/webapps/17[01;31m[K21[m[K3.txt

phpMyChat Plus 1.94 RC1 - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K740.txt
```

phpMyNewsletter 0.6.10 - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K905.txt

PHPMyReports 3.0.11 - 'lib_head.php' Remote File Inclusion
| php/webapps/3[01;31m[K21[m[K2.txt

PHPMyRing 4.2.0 - 'view_com.php' SQL Injection
| php/webapps/[01;31m[K21[m[K59.pl

phpMySport 1.4 - SQL Injection / Authentication Bypass / Full Path Disclosure |
php/webapps/159[01;31m[K21[m[K.txt

PHPNews 1.3 - 'Link_Temp.php' Cross-Site Scripting
| php/webapps/29[01;31m[K21[m[K8.txt

PHPOutsourcing Zorum 3.x - Remote File Inclusion Command Execution
| php/webapps/2[01;31m[K21[m[K95.txt

PHPPass 2 - 'AccessControl.php' SQL Injection
| php/webapps/2[01;31m[K21[m[K48.txt

phpPrintAnalyzer 1.2 - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K68.txt

PHPRank 1.8 - 'add.php' Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K933.txt

PHPReactor 1.2.7 - Style Attribute HTML Injection
| php/webapps/[01;31m[K21[m[K755.txt

PHPReactor 1.2.7 pl1 - 'browse.php' Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K930.txt

PHProjekt 2.x/3.x - Authentication Bypass
| php/webapps/[01;31m[K21[m[K4[01;31m[K21[m[K.txt

PHProjekt 3.1 - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K343.txt

PHProjekt 5.1 - Multiple Remote File Inclusions
| php/webapps/[01;31m[K21[m[K90.txt

phpsyncml 0.1.2 - Remote File Inclusion
| php/webapps/44[01;31m[K21[m[K.txt

PhpTagCool 1.0.3 - SQL Injection
| php/webapps/1[01;31m[K21[m[K1.pl

PhpTax - 'pfilez' Execution Remote Code Injection (Metasploit)
| php/webapps/[01;31m[K21[m[K833.rb

```
phptax 0.8 - Remote Code Execution
| php/webapps/[01;31m[K21[m[K665.txt

phptraverse 0.8.0 - Remote File Inclusion
| php/webapps/10[01;31m[K21[m[K9.txt

PHPWCMS 1.1-RC4 - 'spaw' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K63.txt

phpWebSite 0.10.0 - 'module' SQL Injection
| php/webapps/1[01;31m[K21[m[K7.pl

phpWebSite 0.8.2 - PHP File Inclusion
| php/webapps/[01;31m[K21[m[K825.txt

phpWebSite 0.8.3 - 'article.php' Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K899.txt

phpWebSite 0.8.3 - News Message HTML Injection
| php/webapps/[01;31m[K21[m[K864.txt

Phusion WebServer 1.0 - 'URL' Remote Buffer Overflow
| windows/remote/[01;31m[K21[m[K294.c

Phusion WebServer 1.0 - Directory Traversal (1)
| windows/remote/[01;31m[K21[m[K291.pl

Phusion WebServer 1.0 - Directory Traversal (2)
| windows/remote/[01;31m[K21[m[K292.pl

Phusion WebServer 1.0 - Long URL Denial of Service
| windows/dos/[01;31m[K21[m[K293.pl

Pie Web M{a_e}sher 0.5.3 - Multiple Remote File Inclusions
| php/webapps/72[01;31m[K21[m[K.txt

Pilot Group eTraining - 'lessons_login.php' Cross-Site Scripting
| php/webapps/331[01;31m[K21[m[K.txt

Pimcore 11.4.2 - Stored cross site scripting
| multiple/webapps/5[01;31m[K21[m[K94.py

Pimcore customer-data-framework 4.2.0 -  SQL injection
| multiple/webapps/5[01;31m[K21[m[K93.py

Pine 4.x - 'From:' Heap Corruption
| linux/dos/[01;31m[K21[m[K985.txt

Pine 4.x - Empty MIME Boundary Denial of Service
| unix/dos/[01;31m[K21[m[K644.txt

Pinnacle ShowCenter 1.51 - Web Interface Skin Denial of Service
| php/dos/246[01;31m[K21[m[K.txt
```

Pinterest Clone Script - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K148.txt

Pirch IRC 98 Client - Malformed Link Buffer Overrun
| unix/remote/[01;31m[K21[m[K574.txt

Pirelli ADSL2/2+ Wireless Router P.DGA4001N - Information Disclosure
| hardware/webapps/357[01;31m[K21[m[K.txt

Pivot 1.0 - 'module_db.php' Remote File Inclusion
| php/webapps/24[01;31m[K21[m[K2.txt

Piwigo 2.6.0 - 'picture.php?rate' SQL Injection
| php/webapps/352[01;31m[K21[m[K.txt

Plane 0.23.1 - Server side request forgery (SSRF)
| multiple/webapps/52[01;31m[K21[m[K1.txt

Planet 2.0 - HTML Injection
| php/webapps/33[01;31m[K21[m[K9.txt

PlanetDNS PlanetWeb 1.14 - Remote Buffer Overflow
| linux/remote/[01;31m[K21[m[K945.pl

PlanetWeb 1.14 - GET Buffer Overflow
| windows/dos/[01;31m[K21[m[K795.pl

PlatinumFTPServer 1.0.18 - Multiple Malformed User Name Connection
Denial of Service Vulnerabilities |
windows/dos/25[01;31m[K21[m[K8.pl

PlatinumFTPServer 1.0.6 - Arbitrary File Deletion
| windows/remote/2[01;31m[K21[m[K13.txt

PlatinumFTPServer 1.0.6 - Directory Traversal
| windows/remote/2[01;31m[K21[m[K36.txt

PlatinumFTPServer 1.0.6 - Information Disclosure
| windows/remote/2[01;31m[K21[m[K12.txt

PLC Wireless Router GPN2.4P[01;31m[K21[m[K-C-CN - Arbitrary File
Disclosure |
cgi/webapps/40304.txt

PLC Wireless Router GPN2.4P[01;31m[K21[m[K-C-CN - Cross-Site Request
Forgery |
hardware/webapps/46581.txt

PLC Wireless Router GPN2.4P[01;31m[K21[m[K-C-CN - Cross-Site Scripting
| cgi/webapps/46081.txt

PLC Wireless Router GPN2.4P[01;31m[K21[m[K-C-CN - Denial of Service
| hardware/dos/45187.py

PLC Wireless Router GPN2.4P[01;31m[K21[m[K-C-CN - Incorrect Access Control |
hardware/webapps/46580.txt

PLIB 1.8.5 - 'ssg/ssgParser.cxx' Local Buffer Overflow
| windows/local/[01;31m[K21[m[K831.c

Pligg CMS 9.9.5 - 'CAPTCHA' Registration Automation Security Bypass
| php/webapps/3[01;31m[K21[m[K42.php

Plogger Beta 2.1 - Administrative Credentials Disclosure
| php/webapps/16[01;31m[K21[m[K.php

PLS-Bannieres 1.[01;31m[K21[m[K - 'Bannieres.php' Remote File Inclusion
| php/webapps/28868.txt

Pluck CMS 4.5.2 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K21[m[K68.txt

Plume CMS 1.2.4 - Multiple Local File Inclusions
| php/webapps/1[01;31m[K21[m[K07.txt

PocketPC Mms Composer - 'WAPPush' Denial of Service
| hardware/dos/[01;31m[K21[m[K56.c

Point of Sales (POS) in VB.Net MySQL Database 1.0 - SQL Injection
| php/webapps/457[01;31m[K21[m[K.txt

Police Municipale Open Main Courante 1.01beta - Local File Inclusion / Remote File Inclusion |
php/webapps/1[01;31m[K21[m[K94.txt

Polycom 2.2/3.0 - ViaVideo Buffer Overflow
| windows/dos/[01;31m[K21[m[K941.txt

Polycom ViaVideo 2.2/3.0 - Denial of Service
| hardware/dos/[01;31m[K21[m[K939.txt

Poplar Gedcom Viewer 2.0 - 'common.php' Remote File Inclusion
| php/webapps/31[01;31m[K21[m[K.txt

Portix-PHP 0.4 - 'index.php' Directory Traversal
| php/webapps/[01;31m[K21[m[K277.txt

Portix-PHP 0.4 - 'view.php' Directory Traversal
| php/webapps/[01;31m[K21[m[K278.txt

Portix-PHP 0.4 - Cookie Manipulation
| php/webapps/[01;31m[K21[m[K279.txt

PostBoard 2.0 - BBCode IMG Tag Script Injection
| php/webapps/[01;31m[K21[m[K401.txt

PostBoard 2.0 - Topic Title Script Execution
| php/webapps/[01;31m[K21[m[K403.txt

PostNuke 0.6 - User Login
| php/webapps/[01;31m[K21[m[K119.txt

PostNuke 0.703 - caselist Arbitrary Module Include
| php/webapps/[01;31m[K21[m[K357.txt

PostNuke 0.72 - 'modules.php' Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K873.txt

Power Up HTML 0.8033 Beta - Directory Traversal Arbitrary File
Disclosure |
cgi/remote/[01;31m[K21[m[K102.txt

PowerBook 1.[01;31m[K21[m[K - 'index.php' Local File Inclusion
| php/webapps/5302.txt

PowerDVD 11.0.0.[01;31m[K21[m[K14 - Remote Denial of Service
| windows/dos/36427.txt

PowerDVD 8.0 - '.m3u' / '.pls' Multiple Buffer Overflow Vulnerabilities
| windows/dos/3[01;31m[K21[m[K05.pl

PowerFolder Server 10.4.3[01;31m[K21[m[K - Remote Code Execution
| java/remote/39854.txt

POWERGAP ShopSystem - 's03.php' SQL Injection
| php/webapps/3[01;31m[K21[m[K79.txt

powerUpload 2.4 - (Authentication Bypass) Insecure Cookie Handling
| php/webapps/9[01;31m[K21[m[K9.txt

PowerZip 7.[01;31m[K21[m[K (Build 4010) - Stack Buffer Overflow
| windows/dos/139[01;31m[K21[m[K.c

Powie PForum 1.1x - 'Username' Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K299.txt

pPIM 1.0 - Arbitrary File Delete / Cross-Site Scripting
| php/webapps/6[01;31m[K21[m[K5.txt

PPLive 1.9.[01;31m[K21[m[K - '/LoadModule' URI Handlers Argument
Injection |
windows/remote/8[01;31m[K21[m[K5.txt

pragmaMX Module Landkarten 2.1 (Windows) - Local File Inclusion
| php/webapps/35[01;31m[K21[m[K.pl

Pre Survey Generator - 'default.asp' SQL Injection
| asp/webapps/3[01;31m[K21[m[K11.txt

```
Prisma Industriale Checkweigher PrismaWEB 1.[01;31m[K21[m[K - Hard-
Coded Credentials                                    |
multiple/webapps/44276.txt

Procentia IntelliPen 1.1.12.1520 - 'data.aspx' Blind SQL Injection
| asp/webapps/32[01;31m[K21[m[K2.txt

ProFTPd 1.2.9 rc2 - '.ASCII' File Remote Code Execution (2)
| linux/remote/30[01;31m[K21[m[K.txt

ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)
| linux/remote/169[01;31m[K21[m[K.rb

Progress Database 8.3/9.1 - Multiple Buffer Overflows
| multiple/local/[01;31m[K21[m[K117.txt

Progress Database 9.1 - sqlcpp Local Buffer Overflow
| multiple/local/[01;31m[K21[m[K359.c

Progress Telerik Report Server 2024 Q1 (10.0.24.305) - Authentication
Bypass                                |
multiple/webapps/5[01;31m[K21[m[K03.py

Project Pier - Arbitrary File Upload (Metasploit)
| php/webapps/[01;31m[K21[m[K929.rb

ProjectButler 0.8.4 - 'rootdir' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K83.txt

ProQuiz 2.0.2 - Multiple Vulnerabilities
| php/webapps/204[01;31m[K21[m[K.txt

ProSSHD 1.2 20090726 - Denial of Service (DoS)
| windows/remote/523[01;31m[K21[m[K.NA

Proticaret E-Commerce Script 3.0 - SQL Injection (1)
| multiple/webapps/35[01;31m[K21[m[K9.txt

Prototype of an PHP Application 0.1 - '/ident/loginliste.php?path_inc'
Remote File Inclusion              |
php/webapps/301[01;31m[K21[m[K.txt

Proxomitron Naoko-4 - Cross-Site Scripting
| multiple/remote/[01;31m[K21[m[K025.txt

Psunami Bulletin Board 0.x - 'Psunami.cgi' Remote Command Execution (1)
| cgi/webapps/2[01;31m[K21[m[K69.pl

Psunami Bulletin Board 0.x - 'Psunami.cgi' Remote Command Execution (2)
| cgi/webapps/2[01;31m[K21[m[K70.pl

psyBNC 2.3 - Oversized Passwords Denial of Service
| unix/dos/[01;31m[K21[m[K409.pl
```

```
Pure-FTPd 1.0.[01;31m[K21[m[K (CentOS 6.2 / Ubuntu 8.04) - Null Pointer
Dereference Crash (PoC)                          | linux/dos/20479.pl

PuTTY < 0.68 - 'ssh_agent_channel_data' Integer Overflow Heap
Corruption                                       |
linux/dos/4[01;31m[K21[m[K37.txt

PVote 1.0/1.5 - Poll Content Manipulation
| php/webapps/[01;31m[K21[m[K391.txt

PVote 1.0/1.5 - Unauthorized Administrative Password Change
| php/webapps/[01;31m[K21[m[K397.txt

Py-Membres 3.1 - 'index.php' Unauthorized Access
| php/webapps/[01;31m[K21[m[K886.txt

Python 1.5.2 Pickle - Unsafe 'eval()' Code Execution
| linux/local/[01;31m[K21[m[K623.txt

Python 1.5/1.6/2.0/2.1.x - Pickle Class Constructor Arbitrary Code
Execution                                        |
linux/local/[01;31m[K21[m[K624.py

Python RRDtool Module - Function Format String
| multiple/remote/385[01;31m[K21[m[K.c

PZ Frontend Manager WordPress Plugin 1.0.5 - Cross Site Request Forgery
(CSRF)                                 | php/webapps/5[01;31m[K21[m[K53.NA

Qbik WinGate 6.2.2 - 'LIST' Remote Denial of Service
| multiple/dos/3[01;31m[K21[m[K95.txt

qBittorrent 5.0.1 - MITM RCE
| multiple/local/5[01;31m[K21[m[K90.py

qdPM 7.0 - Arbitrary '.PHP' File Upload (Metasploit)
| php/webapps/[01;31m[K21[m[K835.rb

qmailadmin 1.0.x - Local Buffer Overflow
| linux/local/[01;31m[K21[m[K683.c

QNAP NVR/NAS Devices - Buffer Overflow (PoC)
| hardware/dos/41[01;31m[K21[m[K9.txt

QNAP Turbo NAS TS-1279U-RP - Multiple Path Injections
| hardware/webapps/[01;31m[K21[m[K081.txt

QNX 6.1 - 'TimeCreate' Local Denial of Service
| unix/dos/[01;31m[K21[m[K984.c

QNX 6.4.x/6.5.x ifwatchd - Local Privilege Escalation
| qnx/local/3[01;31m[K21[m[K53.sh
```

QNX 6.4.x/6.5.x pppoectl - Information Disclosure
| qnx/local/3[01;31m[K21[m[K56.txt

QNX 6.5.0 / QCONN 1.4.207944 - Remote Command Execution
| linux/remote/[01;31m[K21[m[K520.py

QNX 6.5.0 x86 io-graphics - Local Privilege Escalation
| qnx/local/3[01;31m[K21[m[K54.c

QNX 6.5.0 x86 phfont - Local Privilege Escalation
| qnx/local/3[01;31m[K21[m[K55.c

QNX 6.x - 'ptrace()' Arbitrary Process Modification
| linux/local/[01;31m[K21[m[K507.sh

QNX QCONN - Remote Command Execution (Metasploit)
| unix/remote/[01;31m[K21[m[K852.rb

QNX RTOS 2.4 - File Disclosure
| linux/local/22[01;31m[K21[m[K2.txt

QNX RTOS 4.25 - 'CRTTrap' File Disclosure
| linux/local/[01;31m[K21[m[K499.txt

QNX RTOS 4.25 - dumper Arbitrary File Modification
| linux/local/[01;31m[K21[m[K501.txt

QNX RTOS 4.25 - monitor Arbitrary File Modification
| linux/local/[01;31m[K21[m[K500.txt

QNX RTOS 4.25/6.1 - 'phgrafx' Local Privilege Escalation
| linux/local/[01;31m[K21[m[K503.sh

QNX RTOS 4.25/6.1 - 'phgrafx-startup' Local Privilege Escalation
| linux/local/[01;31m[K21[m[K504.sh

QNX RTOS 4.25/6.1 - su Password Hash Disclosure
| linux/local/[01;31m[K21[m[K502.txt

QNX RTOS 6.1 - '/usr/photon/bin/phlocale' Environment Variable Buffer
Overflow | linux/local/[01;31m[K21[m[K505.c

QNX RTOS 6.1 - 'PKG-Installer' Local Buffer Overflow
| linux/local/[01;31m[K21[m[K506.c

Qpopper 4.0.x - 'poppassd' Privilege Escalation
| linux/local/[01;31m[K21[m[K.c

QPopper 4.0.x - PopAuth Trace File Shell Command Execution
| unix/remote/[01;31m[K21[m[K185.sh

QQPlayer 3.7.892 - m2p 'quartz.dll' Heap Pointer Overwrite (PoC)
| windows/dos/[01;31m[K21[m[K991.py

```
Qualcomm Eudora 5 - MIME MultiPart Boundary Buffer Overflow
| windows/remote/[01;31m[K21[m[K680.pl

Qualcomm Eudora 5/6 - File Attachment Spoofing (1)
| windows/remote/[01;31m[K21[m[K695.pl

Qualcomm Eudora 5/6 - File Attachment Spoofing (2)
| windows/remote/[01;31m[K21[m[K696.pl

Qualcomm QPopper 4.0.x - Remote Denial of Service
| unix/dos/[01;31m[K21[m[K345.txt

Quate CMS 0.3.4 - Local File Inclusion / Cross-Site Scripting
| php/webapps/6[01;31m[K21[m[K1.txt

Quate CMS 0.3.4 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K21[m[K86.txt

QuestCMS - 'main.php' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K37.txt

Quick.CMS 3.0 - Cross-Site Request Forgery
| php/webapps/17[01;31m[K21[m[K6.txt

Quicksilver Forums 1.4.2 (Windows) - Remote Code Execution
| php/webapps/7[01;31m[K21[m[K7.pl

Quintessential Media Player 5.0.1[01;31m[K21[m[K - '.m3u' Buffer
Overflow                                                  |
windows/dos/34428.py

QwikiWiki 1.5 - 'search.php' Cross-Site Scripting
| php/webapps/27[01;31m[K21[m[K3.txt

Raisecom XPON ISCOMHT803G-U_2.0.0_1405[01;31m[K21[m[K_R4.1.47.002 -
Remote Code Execution                                     |
hardware/webapps/46489.txt

Raptor Firewall 4.0/5.0/6.0.x - Zero Length UDP Packet Resource
Consumption                                  |
windows/dos/[01;31m[K21[m[K143.pl

Rational ClearCase 3.2/4.x - DB Loader TERM Environment Variable Buffer
Overflow                           | unix/local/[01;31m[K21[m[K150.c

Raven Software Soldier Of Fortune 2 - Ignore Command Remote Denial of
Service                                |
windows/dos/259[01;31m[K21[m[K.txt

Ray Chan WWW Authorization Gateway 0.1 - Command Execution
| multiple/remote/191[01;31m[K21[m[K.txt
```

Readymade Classifieds Script 1.0 - SQL Injection
| php/webapps/43[01;31m[K21[m[K2.txt

Real Estate Classifieds Script - SQL Injection
| php/webapps/4[01;31m[K21[m[K67.txt

Real Networks RealJukebox 1.0.2/RealOne 6.0.10 Player Gold - Skinfile
Buffer Overflow |
windows/remote/[01;31m[K21[m[K615.c

RealPlayer 15.0.6.14.3gp - Crash (PoC)
| windows/dos/2[01;31m[K21[m[K54.pl

RealPlayer 7.0/8.0 - Media File Buffer Overflow
| windows/remote/[01;31m[K21[m[K207.c

RealTimes Desktop Service 18.1.4 - 'rpdsvc.exe' Unquoted Service Path
| windows/local/490[01;31m[K21[m[K.txt

ReBB 1.0 - Image Tag Cross-Agent Scripting
| php/webapps/[01;31m[K21[m[K312.txt

Red Mombin 0.7 - 'index.php' Cross-Site Scripting
| php/webapps/287[01;31m[K21[m[K.txt

RedHat 6.2 - Piranha Virtual Server Package Plaintext Password
| linux/local/200[01;31m[K21[m[K.txt

RedHat 6.2/7.0/7.1 Lpd - Remote Command Execution via DVI Printfilter
Configuration Error |
linux/remote/[01;31m[K21[m[K095.txt

RedHat Interchange 4.8.x - Arbitrary File Read
| linux/remote/[01;31m[K21[m[K706.txt

RedHat Linux - Stickiness of /tmp
| linux/dos/16[01;31m[K21[m[K6.txt

RedHat Linux 6.1 i386 - Tmpwatch Recursive Write Denial of Service
| linux/dos/20[01;31m[K21[m[K7.txt

RedHat Linux 7.0 Apache - Remote Username Enumeration
| linux/remote/[01;31m[K21[m[K112.php

RedHat TUX 2.1.0-2 - HTTP Server Oversized Host Denial of Service
| linux/dos/[01;31m[K21[m[K141.txt

Rediff Bol 2.0.2 - URL Handling Denial of Service
| windows/dos/2[01;31m[K21[m[K96.txt

Rediff Bol 7.0 Instant Messenger - ActiveX Control Information
Disclosure |
windows/remote/262[01;31m[K21[m[K.txt

```
reget deluxe 3.0 build 1[01;31m[K21[m[K - Directory Traversal
| jsp/webapps/23872.txt

ReiserFS (Linux Kernel 2.6.34-rc3 / RedHat / Ubuntu 9.10) - 'xattr'
Local Privilege Escalation             |
linux/local/1[01;31m[K21[m[K30.py

reiserfstune 3.6.25 - Local Buffer Overflow
| linux/dos/4[01;31m[K21[m[K10.txt

Rejetto HTTP File Server 2.3m - Remote Code Execution (RCE)
| typescript/webapps/5[01;31m[K21[m[K02.py

Reservic 1.0 - 'id' SQL Injection
| php/webapps/46[01;31m[K21[m[K0.txt

Reservit Hotel 2.1 - Stored Cross-Site Scripting (XSS)
| php/webapps/5[01;31m[K21[m[K33.txt

ResidenceCMS 2.10.1 - Stored Cross-Site Scripting (XSS)
| php/webapps/5[01;31m[K21[m[K50.NA

Respondus for WebCT 1.1.2 - Weak Password Encryption
| multiple/local/[01;31m[K21[m[K078.txt

ReviewPost < 2.84 - Multiple Vulnerabilities
| php/webapps/438[01;31m[K21[m[K.txt

RevilloC MailServer 1.[01;31m[K21[m[K - 'USER' Remote Buffer Overflow
| windows/remote/1565.pl

RGameScript Pro - 'page.php?id' Remote File Inclusion
| php/webapps/4[01;31m[K21[m[K0.txt

RhinoSoft Serv-U FTP Server 7.4.0.1 - 'MKD' Create Arbitrary
Directories                                  |
windows/remote/8[01;31m[K21[m[K1.pl

RhinoSoft Serv-U FTP Server 7.4.0.1 - 'SMNT' (Authenticated) Denial of
Service                              | windows/dos/8[01;31m[K21[m[K2.pl

Rianxosencabos CMS 0.9 - Insecure Cookie Handling
| php/webapps/65[01;31m[K21[m[K.txt

Richard Gooch SimpleInit 2.0.2 - Open File Descriptor
| linux/local/[01;31m[K21[m[K538.c

RICOH Aficio SP 5[01;31m[K21[m[K0SF Printer - 'entryNameIn' HTML
Injection                                                |
hardware/webapps/48164.txt
```

Rit Research Labs The Bat! 1.53 - Microsoft Denial of Service Device Name Denial of Service | windows/dos/[01;31m[K21[m[K307.txt

Riverbed SteelHead VCX 9.6.0a - Arbitrary File Read | linux/webapps/4[01;31m[K21[m[K01.py

RMSOFT Downloads Plus - '/(rmdp) 1.5/1.7 Module for XOOPS down.php?id' Cross-Site Scripting | php/webapps/32[01;31m[K21[m[K6.txt

RMSOFT Downloads Plus - '/(rmdp) 1.5/1.7 Module for XOOPS search.php?key' Cross-Site Scripting | php/webapps/32[01;31m[K21[m[K5.txt

RMSOFT MiniShop 1.0 - 'search.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/3[01;31m[K21[m[K96.txt

Robert 0.5 - Multiple Vulnerabilities | php/webapps/4[01;31m[K21[m[K33.txt

Rogue 5.3 - Local Buffer Overflow | bsd/local/[01;31m[K21[m[K881.txt

RosarioSIS 7.6 - SQL Injection | php/webapps/5[01;31m[K21[m[K69.txt

Rosoft Media Player 4.2.1 (Windows XP SP2/3 French) - Local Buffer Overflow | windows/local/8[01;31m[K21[m[K4.c

Round Cube Webmail 0.1 -200510[01;31m[K21[m[K - Full Path Disclosure | php/webapps/26866.txt

Roundcube Webmail 1.6.6 - Stored Cross Site Scripting (XSS) | php/webapps/5[01;31m[K21[m[K73.txt

Routers2 2.24 - Cross-Site Scripting | perl/webapps/44[01;31m[K21[m[K6.txt

Royal Elementor Addons and Templates 1.3.78 - Unauthenticated Arbitrary File Upload | multiple/webapps/5[01;31m[K21[m[K27.py

RSA Security RSA Authentication Agent For Web 5.2 - Cross-Site Scripting | windows/remote/254[01;31m[K21[m[K.txt

RSMScript 1.[01;31m[K21[m[K - Cross-Site Scripting / Insecure Cookie Handling | php/webapps/7497.txt

```
rsync 2.3/2.4/2.5 - Signed Array Index Remote Code Execution
| linux/remote/[01;31m[K21[m[K242.c

Ruby 1.8.6/1.9 (WEBick HTTPd 1.3.1) - Directory Traversal
| multiple/remote/5[01;31m[K21[m[K5.txt

Ruckus IoT Controller (Ruckus vRIoT) 1.5.1.0.[01;31m[K21[m[K - Remote
Code Execution                                          |
hardware/webapps/49110.py

Rudi Benkovic JAWMail 1.0 - Script Injection
| php/webapps/[01;31m[K21[m[K817.txt

rukovoditel 3.2.1 - Cross-Site Scripting (XSS)
| php/webapps/511[01;31m[K21[m[K.txt

RunCMS 1.6.1 - 'bbPath[root_theme]' Remote File Inclusion
| php/webapps/3[01;31m[K21[m[K00.txt

Ruslan Communications <Body>Builder - Authentication Bypass
| java/webapps/[01;31m[K21[m[K543.txt

RXS-3[01;31m[K21[m[K1 IP Camera - UDP Packet Password Information
Disclosure                                              |
hardware/remote/35800.txt

S8Forum 3.0 - Remote Command Execution
| php/webapps/2[01;31m[K21[m[K34.txt

S9Y Serendipity Freetag-plugin 3.[01;31m[K21[m[K - 'index.php' Cross-
Site Scripting                                          |
php/webapps/35808.txt

SafeNet Sentinel Keys Server - Crash (PoC)
| windows/dos/[01;31m[K21[m[K508.py

SafeTP 1.46 - Passive Mode Internal IP Address Revealing
| multiple/remote/[01;31m[K21[m[K876.txt

Saltstack 3000.1 - Remote Code Execution
| multiple/remote/484[01;31m[K21[m[K.txt

Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploit) (1)
| linux/remote/163[01;31m[K21[m[K.rb

Samba 3.0.[01;31m[K21[m[K < 3.0.24 - LSA trans names Heap Overflow
(Metasploit)                                            |
linux/remote/9950.rb

Samba 3.4.16/3.5.14/3.6.4 - SetInformationPolicy AuditEventsInfo Heap
Overflow (Metasploit)                |
linux/remote/[01;31m[K21[m[K850.rb
```

```
Sambar Server 4.4/5.0 - 'pagecount' File Overwrite
| multiple/remote/[01;31m[K21[m[K026.txt

Sambar Server 4.x/5.0 - Insecure Default Password Protection
| multiple/remote/[01;31m[K21[m[K027.txt

Sambar Server 5.1 - Sample Script Denial of Service
| windows/dos/[01;31m[K21[m[K228.c

Sambar Server 5.1 - Script Source Disclosure
| cgi/remote/[01;31m[K21[m[K390.txt

Sambar Server 5.x - 'results.stm' Cross-Site Scripting
| windows/remote/2[01;31m[K21[m[K85.txt

Samsung ml85p Printer Driver 1.0 - Insecure Temporary File Creation (2)
| hardware/local/[01;31m[K21[m[K000.sh

Samsung ml85p Printer Driver 1.0 - Insecure Temporary File Creation (3)
| hardware/local/[01;31m[K21[m[K001.txt

SAntivirus IC 10.0.[01;31m[K21[m[K.61 - 'SAntivirusIC' Unquoted Service
Path                                                |
windows/local/49042.txt

SantriaCMS - SQL Injection
| php/webapps/18[01;31m[K21[m[K7.txt

SAP NetWeaver - 7.53 - HTTP Request Smuggling
| multiple/remote/5[01;31m[K21[m[K09.txt

SAP NetWeaver Dispatcher - DiagTraceR3Info Buffer Overflow (Metasploit)
| windows/remote/[01;31m[K21[m[K034.rb

SAP SAPCAR 7[01;31m[K21[m[K.510 - Heap Buffer Overflow
| linux/dos/41991.py

SAPID 1.2.3.05 - 'ROOT_PATH' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K28.txt

SAPID Blog Beta 2 - 'ROOT_PATH' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K29.txt

SAPID CMS 1.2.3_rc3 - 'rootpath' Remote Code Execution
| php/webapps/[01;31m[K21[m[K61.pl

SAPID Gallery 1.0 - 'ROOT_PATH' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K30.txt

SAPID Shop 1.2 - 'ROOT_PATH' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K31.txt
```

SapporoWorks Black JumboDog 2.6.4/2.6.5 - HTTP Proxy Buffer Overflow
| windows/remote/[01;31m[K21[m[K[01;31m[K21[m[K4.c

SasCam 2.7 - ActiveX Head Buffer Overflow
| windows/local/14[01;31m[K21[m[K5.txt

Savant Web Server 3.1 - File Disclosure
| windows/remote/[01;31m[K21[m[K794.txt

Savant Web Server 3.1 - Malformed Content-Length Denial of Service
| windows/dos/[01;31m[K21[m[K792.txt

SaveWeb Portal 3.4 - 'SITE_Path' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K13.txt

SaveWebPortal 3.4 - 'page' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K67.txt

Sawmill 6.2.x - Admin Password Insecure Default Permissions
| multiple/local/[01;31m[K21[m[K288.txt

School Faculty Scheduling System 1.0 - Stored Cross Site Scripting POC
| php/webapps/489[01;31m[K21[m[K.txt

School Management System Pro 6.0.0 - Backup Dump
| asp/webapps/12[01;31m[K21[m[K8.txt

Schoolhos CMS Beta 2.29 - 'id' SQL Injection
| php/webapps/2[01;31m[K21[m[K57.txt

Scientific Atlanta DPX[01;31m[K21[m[K00 Cable Modem - LanD Packet
Denial of Service |
hardware/dos/26835.txt

SCPOnly 2.3/2.4 - SSH Environment Shell Escaping
| linux/local/[01;31m[K21[m[K732.txt

ScrewTurn Software ScrewTurn Wiki 2.0.x - 'System Log' Page HTML
Injection |
php/webapps/3[01;31m[K21[m[K26.txt

Scriptme SmE 1.[01;31m[K21[m[K - File Mailer Login SQL Injection
| php/webapps/29474.txt

Seagate Dashboard 4.0.[01;31m[K21[m[K.0 - Crash (PoC)
| windows/dos/37343.py

Seagate Personal Cloud SRN[01;31m[K21[m[KC 4.3.16.0 / 4.3.18.0 - SQL
Injection |
hardware/webapps/45270.txt

Seanox DevWex Windows Binary 1.2002.520 - File Disclosure
| windows/remote/[01;31m[K21[m[K530.txt

```
SecureCRT 2.4/3.x/4.0 - SSH1 Identifier String Buffer Overflow (1)
| windows/dos/[01;31m[K21[m[K634.c

SecureCRT 2.4/3.x/4.0 - SSH1 Identifier String Buffer Overflow (2)
| windows/remote/[01;31m[K21[m[K635.c

Seditio CMS 1[01;31m[K21[m[K - 'pfs.php' Arbitrary File Upload
| php/webapps/4235.txt

Seditio CMS 1[01;31m[K21[m[K - SQL Injection
| php/webapps/4678.php

See-Commerce 1.0.625 - 'owimg.php3' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K55.txt

SEGGER embOS/IP FTP Server 3.22 - Denial of Service
| windows/dos/442[01;31m[K21[m[K.py

SEIG Modbus 3.4 - Denial of Service (PoC)
| windows_x86/dos/45[01;31m[K21[m[K9.py

SEIG SCADA System 9 - Remote Code Execution
| windows_x86/remote/45[01;31m[K21[m[K8.py

SendCard 3.4.0 - Unauthorized Administrative Access
| php/webapps/[01;31m[K21[m[K17.php

Sendmail 8.11/8.12 Debugger - Arbitrary Code Execution (1)
| linux/local/[01;31m[K21[m[K060.c

Sendmail 8.11/8.12 Debugger - Arbitrary Code Execution (2)
| linux/local/[01;31m[K21[m[K061.c

Sendmail 8.11/8.12 Debugger - Arbitrary Code Execution (3)
| linux/local/[01;31m[K21[m[K062.txt

Sendmail 8.11/8.12 Debugger - Arbitrary Code Execution (4)
| linux/local/[01;31m[K21[m[K063.txt

Sendmail 8.12.6 - Compromised Source Backdoor
| unix/remote/[01;31m[K21[m[K919.sh

Sendmail 8.12.x - SMRSH Double Pipe Access Validation
| unix/local/[01;31m[K21[m[K884.txt

Sendmail 8.9.x/8.10.x/8.11.x/8.12.x - File Locking Denial of Service
(1)                                   | linux/dos/[01;31m[K21[m[K476.c

Sendmail 8.9.x/8.10.x/8.11.x/8.12.x - File Locking Denial of Service
(2)                                   | linux/dos/[01;31m[K21[m[K477.c

Seo Panel - 'file' Directory Traversal
| php/webapps/39[01;31m[K21[m[K0.txt
```

Seowon SLR-120 Router - Remote Code Execution (Unauthenticated)
| hardware/remote/508[01;31m[K21[m[K.py

SePortal 2.5 - SQL Injection / Remote Code Execution (Metasploit)
| php/remote/326[01;31m[K21[m[K.rb

Sera 1.2 - Local Privilege Escalation / Password Disclosure
| macos/local/432[01;31m[K21[m[K.sh

ServersCheck Monitoring Software 9.0.12/9.0.14 - Persistent Cross-Site Scripting |
multiple/webapps/[01;31m[K21[m[K866.txt

Sflog! CMS 1.0 - Arbitrary File Upload (Metasploit)
| php/remote/[01;31m[K21[m[K138.rb

SGI IRIX 6.5.4 - midikeys Root
| irix/local/19[01;31m[K21[m[K0.txt

SGI IRIX 6.5.x - FAM Arbitrary Root Owned Directory File Listing
| irix/local/[01;31m[K21[m[K720.txt

SGI IRIX 6.x - 'rpc.xfsmd' Remote Command Execution
| irix/remote/[01;31m[K21[m[K571.c

Shellzip 3.0 Beta 3 - '.zip' Local Stack Buffer Overflow
| windows/local/126[01;31m[K21[m[K.pl

Shop Creator 4.0 - SQL Injection
| asp/webapps/148[01;31m[K21[m[K.txt

ShoutBox 1.2 - 'Form' HTML Injection
| php/webapps/[01;31m[K21[m[K668.txt

SHOUTcast Server 1.9.8/Win32 - Cross-Site Request Forgery
| windows/webapps/11[01;31m[K21[m[K5.txt

Siemens SCALANCE S613 - Remote Denial of Service
| linux/dos/447[01;31m[K21[m[K.py

SilverStripe 5.3.8 - Stored Cross Site Scripting (XSS) (Authenticated)
| multiple/webapps/5[01;31m[K21[m[K99.txt

Sim Editor 6.6 - Local Stack Buffer Overflow
| windows/local/358[01;31m[K21[m[K.txt

Simple CMS - Administrator Authentication Bypass
| php/webapps/[01;31m[K21[m[K33.txt

Simple Image Gallery 1.0 - Remote Code Execution (RCE) (Unauthenticated) |
php/webapps/50[01;31m[K21[m[K4.py

SimpleServer:WWW 1.0.7/1.0.8/1.13 - Hex Encoded URL Directory Traversal
| windows/remote/[01;31m[K21[m[K039.pl

Sitecom Home Storage Center - Authentication Bypass
| hardware/webapps/[01;31m[K21[m[K134.txt

Sitecom Home Storage Center - Directory Traversal
| hardware/webapps/[01;31m[K21[m[K033.txt

Sitecom MD-25x - Multiple Vulnerabilities
| hardware/remote/[01;31m[K21[m[K268.py

SiteGo - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K222.txt

SIX-webboard 2.01 - File Retrieval
| cgi/remote/[01;31m[K21[m[K068.txt

Skype 3.6.[01;31m[K21[m[K6 - Voicemail URI Handler Remote Denial of Service |
multiple/dos/30814.txt

Slackware 7.0/7.1/8.0 - Manual Page Cache File Creation
| linux/local/[01;31m[K21[m[K014.c

SlimCMS 1.0.0 - 'edit.php' SQL Injection
| php/webapps/71[01;31m[K21[m[K.pl

SLIMSV 9.5.2 - Cross-Site Scripting (XSS)
| php/webapps/51[01;31m[K21[m[K1.txt

slocate 2.5/2.6 - Local Buffer Overrun
| linux/dos/2[01;31m[K21[m[K97.txt

SLRNPull 0.9.6 - Spool Directory Command Line Parameter Buffer Overflow
| unix/local/[01;31m[K21[m[K408.pl

Slurp 1.10 - SysLog Remote Format String
| freebsd/dos/[01;31m[K21[m[K512.txt

SmartDesk WebSuite 2.1 - Remote Buffer Overflow
| multiple/remote/192[01;31m[K21[m[K.txt

SmarterMail Build 6985 - Remote Code Execution
| windows/remote/49[01;31m[K21[m[K6.py

Smartfren Connex EC 1261-2 UI OUC - Local Privilege Escalation
| windows/local/[01;31m[K21[m[K547.txt

SmartMail Server 1.0 Beta 10 - Oversized Request Denial of Service
| windows/dos/[01;31m[K21[m[K973.pl

SmartMail Server 2.0 - Closed Connection Denial of Service
| windows/dos/[01;31m[K21[m[K972.pl

SmartMax MailMax 4.8 - Popmax Buffer Overflow
| windows/remote/[01;31m[K21[m[K633.c

SMF 2.0.1 - SQL Injection / Privilege Escalation
| php/webapps/18[01;31m[K21[m[K4.py

SnapStream Personal Video Station 1.2 a - PVS Directory Traversal
| windows/remote/[01;31m[K21[m[K030.txt

SnapStream PVS 1.2 - Plaintext Password
| windows/remote/[01;31m[K21[m[K035.txt

Snes9x 1.3 - Local Buffer Overflow
| unix/local/[01;31m[K21[m[K120.c

sNews - 'index.php' Multiple SQL Injections
| php/webapps/27[01;31m[K21[m[K6.txt

sNews - Comment Body Cross-Site Scripting
| php/webapps/27[01;31m[K21[m[K5.txt

Sniggabo CMS 2.[01;31m[K21[m[K - 'search.php' Cross-Site Scripting
| php/webapps/34079.txt

Snitz Forums 2000 3.0/3.1/3.3 - Image Tag Cross-Agent Scripting
| asp/webapps/[01;31m[K21[m[K308.txt

Snitz Forums 2000 3.1 SR4 - 'pop_profile.asp' SQL Injection
| asp/webapps/33[01;31m[K21[m[K.txt

Snitz Forums 2000 3.x - 'members.asp' SQL Injection
| asp/webapps/[01;31m[K21[m[K400.txt

Snom IP Phone Web Interface < 8 - Multiple Vulnerabilities
| hardware/webapps/17[01;31m[K21[m[K5.txt

Snort 1.8.3 - ICMP Denial of Service
| multiple/dos/[01;31m[K21[m[K[01;31m[K21[m[K3.txt

Snort 2.4.0 - SACK TCP Option Error Handling Denial of Service
| multiple/dos/1[01;31m[K21[m[K3.c

soapbox 0.3.1 - Local Privilege Escalation
| linux/local/[01;31m[K21[m[K666.txt

Social News and Bookmarking Script - SQL Injection
| php/webapps/411[01;31m[K21[m[K.txt

Social Share - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/351[01;31m[K21[m[K.txt

Softbiz Image Gallery - 'adminhome.php?msg' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K74.txt

Softbiz Image Gallery - 'browsecats.php?msg' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K78.txt

Softbiz Image Gallery - 'changepassword.php?msg' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K76.txt

Softbiz Image Gallery - 'cleanup.php?msg' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K77.txt

Softbiz Image Gallery - 'config.php?msg' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K75.txt

Softbiz Image Gallery - 'images.php' Multiple Cross-Site Scripting
Vulnerabilities |
php/webapps/3[01;31m[K21[m[K71.txt

Softbiz Image Gallery - 'image_desc.php?latest' Cross-Site Scripting
| php/webapps/3[01;31m[K21[m[K73.txt

Softbiz Image Gallery - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities |
php/webapps/3[01;31m[K21[m[K70.txt

Softbiz Image Gallery - 'suggest_image.php' Multiple Cross-Site
Scripting Vulnerabilities |
php/webapps/3[01;31m[K21[m[K72.txt

SoftComplex PHP Image Gallery 1.0 - Authentication Bypass
| php/webapps/70[01;31m[K21[m[K.txt

Softek MailMarshal 4 / Trend Micro ScanMail 1.0 - SMTP Attachment
Protection Bypass |
multiple/remote/[01;31m[K21[m[K029.pl

software602 602 lan suite 2004 - Directory Traversal
| windows/remote/256[01;31m[K21[m[K.txt

Software602 602 Lan Suite 2004 2004.0.04.12[01;31m[K21[m[K - Arbitrary
File Upload |
windows/remote/25092.txt

Solaris 2.6/7.0 - 'locale' Format Strings noexec stack Overflow
| solaris/local/[01;31m[K21[m[K0.c

Solaris 2.6/7.0 - DTMail Mail Environment Variable Buffer Overflow
| solaris/local/[01;31m[K21[m[K024.c

Solaris 2.6/7/8 (SPARC) - xlock Heap Overflow
| solaris/local/[01;31m[K21[m[K058.c

```
Solaris 2.x/7.0/8 - 'Catman' Race Condition (2)
| solaris/local/205[01;31m[K21[m[K.pl

Solaris 2.x/7.0/8 - Derived 'login' Remote Buffer Overflow
| solaris/remote/[01;31m[K21[m[K179.pl

Solaris 2.x/7.0/8 / IRIX 6.5.x / OpenBSD 2.x / NetBSD 1.x / Debian 3 /
HP-UX 10 - 'TelnetD' Remote Buffer  | unix/remote/[01;31m[K21[m[K018.c

Solaris 2.x/7.0/8 LPD - Remote Command Execution
| solaris/remote/[01;31m[K21[m[K097.txt

Solaris 2/7/8/9 cachefsd - Remote Heap Overflow
| solaris/remote/[01;31m[K21[m[K437.c

Solaris 7.0/8 Sunsolve CD - SSCD_SunCourier.pl CGI Script Arbitrary
Command Execution                     |
cgi/remote/[01;31m[K21[m[K340.pl

Solaris 8 - x86 xlock Heap Overflow
| solaris/local/[01;31m[K21[m[K059.c

Solaris 8.0 LPD - Command Execution (Metasploit)
| solaris/remote/99[01;31m[K21[m[K.rb

Solaris sadmind - Remote Buffer Overflow
| solaris/remote/[01;31m[K21[m[K3.c

SolarWinds TFTP Server Standard Edition 5.0.55 - Directory Traversal
| windows/remote/[01;31m[K21[m[K964.txt

SolarWinds TFTP Server Standard Edition 5.0.55 - Large UDP Packet
| windows/dos/[01;31m[K21[m[K963.pl

SolidWorks Workgroup PDM 2014 - 'pdmwService.exe' Arbitrary File Write
(Metasploit)                          |
windows/remote/3[01;31m[K21[m[K63.rb

Solstice Pod 6.2 - API Session Key Extraction via API Endpoint
| windows/local/5[01;31m[K21[m[K04.txt

SOMPL Player 1.0 - Local Buffer Overflow
| windows/local/11[01;31m[K21[m[K9.pl

Sonatype Nexus 3.[01;31m[K21[m[K.1 - Remote Code Execution
(Authenticated)                                                 |
java/webapps/49385.py

Sonatype Nexus Repository 3.53.0-01 - Path Traversal
| multiple/webapps/5[01;31m[K21[m[K01.py

Sonicwall < 8.1.0.6-[01;31m[K21[m[Ksv - 'gencsr.cgi' Command Injection
(Metasploit)                                    | cgi/webapps/42343.rb
```

SonicWALL email security 7.3.5 - Multiple Vulnerabilities
| windows/webapps/[01;31m[K21[m[K394.txt

SonicWall NetExtender 10.2.0.300 - Unquoted Service Path
| windows/local/50[01;31m[K21[m[K2.txt

SonicWALL SOHO3 6.3 - Content Blocking Script Injection
| multiple/remote/[01;31m[K21[m[K453.txt

Sonium Enterprise Adressbook 0.2 - 'folder' Include
| php/webapps/2[01;31m[K21[m[K6.txt

Sony XAV-AX5500 1.13 - Firmware Update Validation Remote Code Execution
(RCE) |
multiple/remote/5[01;31m[K21[m[K43.py

Soritong MP3 Player 1.0 - 'SKIN' Local Stack Overflow (SEH)
| windows/local/9[01;31m[K21[m[K6.pl

SourceBans 1.4.8 - SQL Injection / Local File Inclusion Injection
| php/webapps/18[01;31m[K21[m[K5.txt

Spaminator 1.7 - 'page' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K65.txt

SpeechD 0.1/0.2 - Privileged Command Execution
| unix/local/[01;31m[K21[m[K108.txt

SPGPartenaires 3.0.1 - 'delete.php' SQL Injection
| php/webapps/2[01;31m[K21[m[K08.txt

SPGPartenaires 3.0.1 - 'ident.php' SQL Injection
| php/webapps/2[01;31m[K21[m[K07.txt

SpiceWorks 6.0.00993 - Multiple Script Injection Vulnerabilities
| windows/webapps/[01;31m[K21[m[K392.txt

Spidey Blog Script 1.5 - 'proje_goster.asp' SQL Injection (1)
| asp/webapps/[01;31m[K21[m[K86.txt

Spidey Blog Script 1.5 - 'proje_goster.asp' SQL Injection (2)
| asp/webapps/24[01;31m[K21[m[K.pl

Spinworks Application Server 3.0 - Remote Denial of Service
| windows/dos/25[01;31m[K21[m[K9.txt

Spitfire 1.0.381 - Cross-Site Scripting / Cross-Site Request Forgery
| php/webapps/343[01;31m[K21[m[K.txt

Splatt Forum 3.0 - Image Tag HTML Injection
| php/webapps/[01;31m[K21[m[K514.txt

```
Splunk 4.3.3 - Arbitrary File Read
| multiple/webapps/[01;31m[K21[m[K053.txt

SpoonFTP 1.2 - RETR Denial of Service
| windows/dos/170[01;31m[K21[m[K.py

SpotIM 2.2 - Denial of Service (PoC)
| windows/dos/468[01;31m[K21[m[K.py

SQL Monitor 12.1.31.893 - Cross-Site Scripting (XSS)
| multiple/webapps/51[01;31m[K21[m[K8.txt

SQLiteWebAdmin 0.1 - 'tpl.inc.php' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K23.txt

Squid 2.0-4 - Cache FTP Proxy URL Buffer Overflow
| unix/remote/[01;31m[K21[m[K297.c

Squid < 3.1 5 - HTTP Version Number Parsing Denial of Service
| multiple/dos/80[01;31m[K21[m[K.pl

Squid Web Proxy 2.3 - Reverse Proxy
| linux/remote/[01;31m[K21[m[K017.txt

SquirrelMail 1.2.6/1.2.7 - Multiple Cross-Site Scripting
Vulnerabilities                                      |
php/webapps/[01;31m[K21[m[K811.txt

SquirrelMail 1.2.x - Theme Remote Command Execution
| php/webapps/[01;31m[K21[m[K358.sh

SSGBook 1.0 - Image Tag HTML Injection
| asp/webapps/[01;31m[K21[m[K914.txt

SSH2 3.0 - Restricted Shell Escape (Command Execution)
| linux/local/[01;31m[K21[m[K398.txt

SSH2 3.0 - Short Password Login
| unix/remote/[01;31m[K21[m[K0[01;31m[K21[m[K.pl

Steamcast - HTTP Request Remote Buffer Overflow (SEH) (1)
| windows/remote/84[01;31m[K21[m[K.py

Stoney FTPd - 'rxBot mods ftpd' Denial of Service
| windows/dos/1[01;31m[K21[m[K8.c

Streaming Audio Player 0.9 - 'skin' Local Stack Overflow (SEH)
| windows/local/9[01;31m[K21[m[K5.pl

STunnel 3.x - Client Negotiation Protocol Format String
| linux/remote/[01;31m[K21[m[K192.c
```

```
Subex Fms 7.4 - SQL Injection
| multiple/webapps/35[01;31m[K21[m[K4.txt

Subrion CMS 2.2.1 - Cross-Site Request Forgery (Add Admin)
| php/webapps/[01;31m[K21[m[K267.txt

subrion CMS 2.2.1 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K21[m[K59.txt

Subsonic 6.1.1 - Cross-Site Request Forgery
| windows/webapps/4[01;31m[K21[m[K17.txt

Subsonic 6.1.1 - Cross-Site Request Forgery / Cross-Site Scripting
| windows/webapps/4[01;31m[K21[m[K20.txt

Subsonic 6.1.1 - Server-Side Request Forgery
| windows/webapps/4[01;31m[K21[m[K18.txt

Subsonic 6.1.1 - XML External Entity Injection
| windows/local/4[01;31m[K21[m[K19.txt

Subtitle Processor 7.7.1 - Local Buffer Overflow (SEH Unicode)
| windows/local/17[01;31m[K21[m[K7.py

Sudo 1.6.3 - Unclean Environment Variable Privilege Escalation
| linux/local/[01;31m[K21[m[K227.sh

Sudo 1.6.x - Password Prompt Heap Overflow
| linux/local/[01;31m[K21[m[K420.c

sudo 1.8.0 to 1.9.12p1 - Privilege Escalation
| linux/local/51[01;31m[K21[m[K7.sh

Sudo 1.8.20 - 'get_process_ttyname()' Local Privilege Escalation
| linux/local/4[01;31m[K21[m[K83.c

Sudo 1.9.5p1 - 'Baron Samedit ' Heap-Based Buffer Overflow Privilege
Escalation (1)                          |
multiple/local/495[01;31m[K21[m[K.py

SugarCRM Community Edition 4.5.1/5.0.0 - File Disclosure
| php/webapps/55[01;31m[K21[m[K.txt

Summit Computer Networks Lil' HTTP Server 2 - 'URLCount.cgi' HTML
Injection                                    |
windows/remote/[01;31m[K21[m[K581.txt

Summit Computer Networks Lil' HTTP Server 2.1/2.2 - 'pbcgi.cgi' Cross-
Site Scripting                           |
windows/remote/[01;31m[K21[m[K611.txt

Sun AnswerBook2 1.x - Unauthorized Administrative Script Access
| solaris/remote/[01;31m[K21[m[K677.txt
```

Sun Cobalt RaQ 1.1/2.0/3.0/4.0 - 'Message.cgi' Cross-Site Scripting
| cgi/webapps/23[01;31m[K21[m[K4.txt

Sun Cobalt RaQ 4.0 - Predictable Temporary Filename Symbolic Link
Attack |
linux/local/[01;31m[K21[m[K733.sh

Sun i-Runbook 2.5.2 - Directory and File Content Disclosure
| php/webapps/[01;31m[K21[m[K610.txt

Sun Java System Messenger Express 6.1-13-15 - 'sid' Cross-Site
Scripting |
java/webapps/316[01;31m[K21[m[K.txt

Sun Java Virtual Machine 1.2.2/1.3.1 - Segmentation Violation
| linux/local/[01;31m[K21[m[K259.java

Sun Microsystems Solaris SRSEXEC 3.2.x - Arbitrary File Read Local
Information Disclosure |
solaris/local/300[01;31m[K21[m[K.txt

Sun ONE Starter Kit 2.0 / ASTAware SearchDisc 3.1 - Search Engine
Directory Traversal |
java/webapps/[01;31m[K21[m[K879.txt

Sun ONE Unified Development Server 5.0 - Recursive Document Type
Definition |
multiple/remote/2[01;31m[K21[m[K78.xml

Sun Solaris 2.5.1/2.6/7.0/8/9 Wall - Spoofed Message Origin
| solaris/local/2[01;31m[K21[m[K20.c

Sun Solaris 2.6/7.0/8 - XSun Color Database File Heap Overflow
| solaris/local/[01;31m[K21[m[K360.c

Sun SunPCi II VNC Software 2.3 - Password Disclosure
| unix/local/[01;31m[K21[m[K592.c

Sun xVM VirtualBox < 1.6.4 - Privilege Escalation (PoC)
| multiple/dos/6[01;31m[K21[m[K8.txt

Sungard eTRAKiT3 <= 3.2.1.17 - SQL Injection
| json/webapps/4[01;31m[K21[m[K11.txt

SunShop Shopping Cart 1.5/2.x - User-Embedded Scripting
| php/webapps/[01;31m[K21[m[K377.txt

Sunway Force Control SCADA 6.1 SP3 - 'httpsrv.exe' Remote Overflow
| windows/remote/177[01;31m[K21[m[K.rb

Super Site Searcher - Remote Command Execution
| cgi/webapps/[01;31m[K21[m[K768.txt

Support4Arabs Pages 2.0 - SQL Injection
| php/webapps/[01;31m[K21[m[K054.txt

SurfControl SuperScout Email Filter 3.5 - 'MsgError.asp' Cross-Site Scripting |
asp/webapps/[01;31m[K21[m[K924.txt

SurfControl SuperScout Email Filter 3.5 - User Credential Disclosure
| asp/webapps/[01;31m[K21[m[K925.txt

SurfControl SuperScout WebFilter for Windows 2000 - File Disclosure
| windows/remote/[01;31m[K21[m[K897.txt

SurfControl SuperScout WebFilter for Windows 2000 - SQL Injection
| windows/remote/[01;31m[K21[m[K898.txt

SuSE 6.3/6.4/7.0 sdb - Arbitrary Command Execution
| linux/remote/[01;31m[K21[m[K075.txt

SuSE Linux 6.4/7.0/7.1/7.2 Berkeley Parallel Make - Local Buffer Overflow |
linux/local/[01;31m[K21[m[K159.c

SuSE Linux 6.4/7.0/7.1/7.2 Berkeley Parallel Make - Shell Definition Format String |
linux/local/[01;31m[K21[m[K158.c

SWS Simple Web Server 0.0.3/0.0.4/0.1 - New Line Denial of Service
| linux/dos/[01;31m[K21[m[K775.c

Symantec Enterprise Firewall 7.0/8.0 - DNSD DNS Cache Poisoning
| windows/remote/24[01;31m[K21[m[K8.cpp

Symantec Java! JustInTime Compiler [01;31m[K21[m[K0.65 - Command Execution |
windows/remote/22028.txt

Symantec Messaging Gateway 9.5/9.5.1 - SSH Default Password Security Bypass (Metasploit) |
linux/remote/[01;31m[K21[m[K136.rb

Symantec Norton Internet Security 2003 - ICMP Packet Flood Denial of Service |
windows/dos/2[01;31m[K21[m[K62.txt

Symantec Norton Personal Firewall 2002/Kaspersky Labs Anti-Hacker 1.0/BlackIce Server Protection 3.5/Black |
windows/dos/[01;31m[K21[m[K915.txt

Symantec Workspace Streaming - Arbitrary File Upload (Metasploit)
| multiple/remote/335[01;31m[K21[m[K.rb

```
Symphony CMS 2.1.2 - Blind SQL Injection
| php/webapps/17[01;31m[K21[m[K8.txt

Sync Breeze 9.7.26 - 'Add Exclude Directory' Local Buffer Overflow
| windows/local/4[01;31m[K21[m[K61.py

SysInfo 1.[01;31m[K21[m[K - 'sysinfo.cgi' Remote Command Execution
| cgi/webapps/1677.php

Tagger Luxury Edition - 'BBCodeFile' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K57.txt

TANne 0.6.17 - Session Manager SysLog Format String
| linux/remote/2[01;31m[K21[m[K35.c

Tarantella Enterprise 3 - gunzip Race Condition
| unix/local/[01;31m[K21[m[K244.pl

Tarantella Enterprise 3 - Symbolic Link
| unix/local/[01;31m[K21[m[K290.sh

Tastydir 1.2 (1[01;31m[K21[m[K6) - Multiple Vulnerabilities
| php/webapps/15269.txt

Taylor UUCP 1.0.6 - Argument Handling Privilege Escalation
| unix/local/[01;31m[K21[m[K106.txt

TBK DVR4104 / DVR4[01;31m[K21[m[K6 - Credentials Leak
| hardware/remote/44577.py

TeamPass 3.0.0.[01;31m[K21[m[K - SQL Injection
| php/webapps/52094.py

Techno Portfolio Management Panel - 'id' SQL Injection
| php/webapps/43[01;31m[K21[m[K1.txt

Teekai Tracking Online 1.0 - Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K509.txt

TelCondex SimpleWebserver 2.0.6 - Denial of Service
| windows/dos/[01;31m[K21[m[K938.txt

TelCondex SimpleWebserver 2.12.30[01;31m[K21[m[K0 build 3285 - HTTP
Referer Remote Buffer Overflow                      |
windows/dos/23310.pl

Telindus 1100 Series Router - Administration Password Leak
| hardware/remote/[01;31m[K21[m[K513.c

Tembria Server Monitor 5.6.0 - Denial of Service
| windows/dos/1[01;31m[K21[m[K31.py
```

```
Template CMS 2.1.1 - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K742.txt

TerraMaster TOS 4.2.06 - RCE (Unauthenticated)
| linux/webapps/493[01;31m[K21[m[K.py

TestLink 1.9.3 - Cross-Site Request Forgery
| php/webapps/[01;31m[K21[m[K135.txt

TFTPD32 < 2.[01;31m[K21[m[K - 'Filename' Remote Buffer Overflow
(Metasploit)                                                |
windows/remote/16349.rb

Thatware 0.4.6 - 'ROOT_PATH' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K66.txt

Thatware 0.4.6 - SQL Injection
| php/webapps/405[01;31m[K21[m[K.txt

Thomson Wireless VoIP Cable Modem - Authentication Bypass
| hardware/webapps/[01;31m[K21[m[K417.py

Thunderstone TEXIS 3.0 - Full Path Disclosure
| multiple/remote/[01;31m[K21[m[K276.txt

Tibco ObfuscationEngine 5.11 - Fixed Key Password Decryption
| multiple/local/492[01;31m[K21[m[K.java

TightAuction 3.0 - Config.INC Information Disclosure
| php/webapps/[01;31m[K21[m[K893.php

Tiki Wiki CMS Groupware [01;31m[K21[m[K.1 - Authentication Bypass
| php/webapps/48927.py

TinyPHP Forum 3.6 - 'makeAdmin' Remote Admin Maker
| php/webapps/[01;31m[K21[m[K14.html

TinyWebGallery 1.5 - 'image' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K58.txt

TIPS MailPost 5.1.1 - 'APPEND' Cross-Site Scripting
| cgi/webapps/247[01;31m[K21[m[K.txt

TitanFTP 2.0.1.[01;31m[K21[m[K02 - Path traversal to Remote Code
Execution (RCE)                                             |
windows/remote/51268.txt

Tolva 0.1 - 'Usermods.php' Remote File Inclusion
| php/webapps/269[01;31m[K21[m[K.txt

TomatoCart 1.2.0 Alpha 2 - 'json.php' Local File Inclusion
| php/webapps/370[01;31m[K21[m[K.txt
```

Torbstoff News 4 - 'pfad' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K[01;31m[K21[m[K.txt

torrenttrader 2.08 - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K396.txt

Total Video Player - 'vcen.dll' Remote Off-by-One Crash
| windows/dos/7[01;31m[K21[m[K9.pl

TP-Link Archer AX[01;31m[K21[m[K - Unauthenticated Command Injection
| hardware/remote/51677.py

TP-Link Router AX50 firmware [01;31m[K21[m[K0730 - Remote Code
Execution (RCE) (Authenticated) |
hardware/remote/50962.py

TP-Link TL-WR902AC firmware [01;31m[K21[m[K0730 (V3) - Remote Code
Execution (RCE) (Authenticated) |
hardware/remote/51192.py

TP-Link VN020 F3v(T) TT_V6.2.10[01;31m[K21[m[K - Buffer Overflow Memory
Corruption |
multiple/remote/52249.c

TP-Link VN020 F3v(T) TT_V6.2.10[01;31m[K21[m[K - Denial Of Service
(DOS) |
multiple/remote/52250.txt

TP-Link VN020 F3v(T) TT_V6.2.10[01;31m[K21[m[K) - DHCP Stack Buffer
Overflow |
multiple/local/52292.c

tplSoccerStats - 'player.php' SQL Injection
| php/webapps/16[01;31m[K21[m[K4.txt

Traq 2.3 - Authentication Bypass / Remote Code Execution
| php/webapps/18[01;31m[K21[m[K3.php

Trellian FTP Client - PASV Buffer Overflow
| windows/remote/1[01;31m[K21[m[K52.pl

Trend Micro - node.js HTTP Server Listening on localhost Can Execute
Commands |
windows/remote/39[01;31m[K21[m[K8.html

Trend Micro Anti-Threat Toolkit 1.62.0.1[01;31m[K21[m[K8 - Remote Code
Execution |
windows/local/47527.txt

Trend Micro Control Manager 5.5/6.0 AdHocQuery - (Authenticated) Blind
SQL Injection |
windows/webapps/[01;31m[K21[m[K546.py

Trend Micro Interscan Messaging Security Suite - Persistent Cross-Site Scripting / Cross-Site Request Forg | aix/webapps/[01;31m[K21[m[K319.txt

Trend Micro Interscan VirusWall 3.5/3.6 - Content-Length Scan Bypass | multiple/remote/[01;31m[K21[m[K339.c

Trend Micro Interscan VirusWall for Windows NT 3.52 - Space Gap Scan Bypass | windows/remote/[01;31m[K21[m[K625.pl

Trend Micro OfficeScan 3.x - CGI Directory Insufficient Permissions | windows/remote/2[01;31m[K21[m[K71.txt

Trend Micro ScanMail For Exchange 3.8 - Authentication Bypass | windows/remote/2[01;31m[K21[m[K74.txt

Trend Micro Virtual Mobile Infrastructure 5.5.1336 - 'Server address' Denial of Service (PoC) | ios/dos/453[01;31m[K21[m[K.py

Trend Micro Virus Control System 1.8 - Denial of Service | windows/dos/2[01;31m[K21[m[K72.txt

Trend Micro Virus Control System 1.8 - Information Disclosure | windows/remote/2[01;31m[K21[m[K73.txt

Trend Micro VirusWall 3.81 - 'vscan/VSAPI' Local Buffer Overflow | linux/local/3[01;31m[K21[m[K3.c

TRENDnet SecurView TV-IP1[01;31m[K21[m[KWN Wireless Internet Camera - UltraMJCam ActiveX Control OpenFileDlg WideCharTo | hardware/remote/18675.txt

Trillian 0.6351/0.7x - Identd Buffer Overflow | windows/remote/[01;31m[K21[m[K804.c

Trillian 0.725/0.73/0.74 - IRC User Mode Numeric Remote Buffer Overflow | windows/dos/[01;31m[K21[m[K816.c

Trillian 0.73/0.74 - IRC JOIN Buffer Overflow | windows/dos/[01;31m[K21[m[K813.c

Trillian 0.73/0.74 - IRC PRIVMSG Buffer Overflow | windows/remote/[01;31m[K21[m[K810.c

Trillian 0.74 - IRC Oversized Data Block Buffer Overflow | windows/dos/[01;31m[K21[m[K823.c

Trillian 0.74 - IRC PART Message Denial of Service | windows/dos/[01;31m[K21[m[K8[01;31m[K21[m[K.c

Trillian 0.74 - IRC Raw Messages Denial of Service | windows/dos/[01;31m[K21[m[K819.c

```
Trillian 0.x IRC Module - Remote Buffer Overflow
| windows/remote/[01;31m[K21[m[K675.pl

Trillian Instant Messaging 0.x - Credential Encryption
| windows/local/[01;31m[K21[m[K781.c

Tru64 - Malformed TCP Packet Denial of Service
| unix/dos/[01;31m[K21[m[K261.txt

TSEP 0.942 - 'colorswitch.php' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K16.txt

Tunez 1.[01;31m[K21[m[K - 'search.php?searchFor' Cross-Site Scripting
| php/webapps/26566.txt

Tunez 1.[01;31m[K21[m[K - 'songinfo.php?song_id' SQL Injection
| php/webapps/26565.txt

Turbo FTP Server 1.30.823 - PORT Overflow (Metasploit)
| windows/remote/2[01;31m[K21[m[K61.rb

TWiki 4.0.4 - 'configure' Remote Command Execution
| php/webapps/[01;31m[K21[m[K43.pl

TWiki 4.0.4 - Configure Script Remote Code Execution (Metasploit)
| php/webapps/[01;31m[K21[m[K10.pm

Typecho 1.3.0 - Race Condition
| php/webapps/5[01;31m[K21[m[K61.go

Typecho 1.3.0 - Stored Cross-Site Scripting (XSS)
| php/webapps/5[01;31m[K21[m[K62.go

UBBCentral UBB.Threads 5.5.1 - 'message' SQL Injection
| php/webapps/8[01;31m[K21[m[K0.txt

UBBCentral UBB.Threads 6.0 - 'editpost.php' SQL Injection
| php/webapps/25[01;31m[K21[m[K2.txt

Ubisoft uplay 2.0.3 - ActiveX Control Arbitrary Code Execution
(Metasploit)                                |
windows/remote/203[01;31m[K21[m[K.rb

Ultimate Bulletin Board 5.4/6.0/6.2 - Cross-Agent Scripting
| cgi/webapps/[01;31m[K21[m[K209.txt

Ultimate PHP Board 1.0/1.1 - Image Tag Script Injection
| php/webapps/[01;31m[K21[m[K423.txt

Ultimate PHP Board 2.0 - 'header_simple.php' File Inclusion
| php/webapps/27[01;31m[K21[m[K.php
```

Ultra Mini HTTPd 1.[01;31m[K21[m[K - 'POST' Remote Stack Buffer Overflow (1) | windows/remote/31736.py

Ultra Mini HTTPd 1.[01;31m[K21[m[K - 'POST' Remote Stack Buffer Overflow (2) | windows/remote/31814.py

Ultra Mini HTTPd 1.[01;31m[K21[m[K - Remote Stack Buffer Overflow | windows/remote/26739.py

UltraEdit 8.2 - FTP Client Weak Password Encryption | windows/local/[01;31m[K21[m[K091.txt

Ultrafunk Popcorn 1.20 - Multiple Denial of Service Vulnerabilities | windows/dos/[01;31m[K21[m[K612.txt

UNA 10.0.0 RC1 - 'polyglot.php' Persistent Cross-Site Scripting | php/webapps/472[01;31m[K21[m[K.txt

UNA CMS 14.0.0-RC - PHP Object Injection | multiple/webapps/5[01;31m[K21[m[K39.txt

UNAK-CMS 1.5 - 'connector.php' Local File Inclusion | php/webapps/3[01;31m[K21[m[K50.txt

Unijimpe Captcha - 'captchademo.php' Cross-Site Scripting | php/webapps/37[01;31m[K21[m[K6.txt

Uniview NVR - Password Disclosure | hardware/webapps/4[01;31m[K21[m[K50.py

Unreal Commander 0.92 - ZIP / RAR Archive Handling Traversal Arbitrary File Overwrite | multiple/remote/305[01;31m[K21[m[K.txt

Unreal Tournament 2004 - Null Pointer Remote Denial of Service | multiple/dos/3[01;31m[K21[m[K25.txt

Unreal Tournament 3 - Memory Corruption (Denial of Service) | multiple/dos/3[01;31m[K21[m[K27.txt

UoW Pine 4.0.4/4.10/4.[01;31m[K21[m[K - 'From:' Remote Buffer Overflow | linux/remote/20237.c

UPS Web/SNMP-Manager CS1[01;31m[K21[m[K - Authentication Bypass | multiple/remote/39186.pl

User-Mode Linux (Linux Kernel 2.4.17-8) - Memory Access Privilege Escalation | linux/local/[01;31m[K21[m[K248.txt

```
UTstarcom WA3002G4 - DNS Change
| hardware/webapps/4[01;31m[K21[m[K94.sh

UUCP - File Creation/Overwriting Symlinks
| linux/local/[01;31m[K21[m[K7.c

V-EVA Classified Script 5.1 - 'classified_img.php' SQL Injection
| php/webapps/34[01;31m[K21[m[K8.txt

Vacation Rental Script 3.0 - 'id' SQL Injection
| php/webapps/62[01;31m[K21[m[K.txt

Valentina Studio 9.0.4 - 'Host' Denial of Service (PoC)
| windows/dos/464[01;31m[K21[m[K.py

vAuthenticate 2.8 - SQL Injection
| php/webapps/2[01;31m[K21[m[K67.txt

vBulletin (Cyb - Advanced Forum Statistics) - 'misc.php' Denial of
Service                                  |
php/dos/1[01;31m[K21[m[K54.txt

vBulletin 2.0.3 - 'calendar.php' Command Execution
| php/webapps/[01;31m[K21[m[K874.txt

vBulletin 2.0/2.2.x - Cross-Site Scripting
| java/webapps/[01;31m[K21[m[K946.txt

vBulletin 5 - 'index.php/ajax/api/reputation/vote?nodeid' SQL Injection
(Metasploit)                       | php/remote/30[01;31m[K21[m[K2.rb

vBulletin Adsense Component - 'viewpage.php' SQL Injection
| php/webapps/336[01;31m[K21[m[K.txt

VBZoom 1.0 - Arbitrary File Upload
| php/webapps/[01;31m[K21[m[K9[01;31m[K21[m[K.txt

VBZoom 1.0 - SQL Injection
| php/webapps/[01;31m[K21[m[K918.html

vCard PRO - 'create.php?card_id' SQL Injection
| php/webapps/281[01;31m[K21[m[K.txt

VCDGear 3.56 Build 050[01;31m[K21[m[K3 - 'FILE' Local Code Execution
| windows/local/3727.c

Veritas NetBackup 4/5 - Volume Manager Daemon Remote Buffer Overflow
| windows/remote/14[01;31m[K21[m[K.cpp

Versant Object Database 7.0.1.3 - Commands Execution
| windows/remote/5[01;31m[K21[m[K3.txt
```

VestaCP 0.9.8-26 - 'LoginAs' Insufficient Session Validation
| multiple/webapps/49[01;31m[K21[m[K9.txt

VFS for Git 1.0.[01;31m[K21[m[K014.1 - 'GVFS.Service' Unquoted Service Path |
windows/local/49661.txt

Viap Automation WinPLC7 5.0.45.59[01;31m[K21[m[K - Recv Buffer Overflow (Metasploit) |
windows/remote/42693.rb

ViArt Shop Enterprise 4.1 - Arbitrary Command Execution
| php/webapps/[01;31m[K21[m[K5[01;31m[K21[m[K.txt

ViArt Shop Evaluation 4.1 - Multiple Remote File Inclusions
| php/webapps/[01;31m[K21[m[K524.txt

VICIDIAL Call Center Suite 2.2.1-237 - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K220.txt

VideoLAN VLC Media Player 0.9.8a - Web UI 'input' Remote Denial of Service |
windows/dos/8[01;31m[K21[m[K3.pl

VideoLAN VLC Media Player 2.0.3 - '.png' ReadAV Crash (PoC)
| windows/dos/[01;31m[K21[m[K889.pl

VideoScript 3.0 < 4.0.1.50 - 'Official' Shell Injection
| php/webapps/7[01;31m[K21[m[K1.php

VideoScript 3.0 < 4.1.5.55 - 'Unofficial' Shell Injection
| php/webapps/7[01;31m[K21[m[K2.php

Vieassociative Openmairie 1.01 Beta - Local File Inclusion / Remote File Inclusion |
php/webapps/1[01;31m[K21[m[K87.txt

ViewCVS 0.9.2 - Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K473.txt

Virtual Host Administrator 0.1 - Modules_Dir Remote File Inclusion
| php/webapps/295[01;31m[K21[m[K.txt

Visual Basic - 'vbe6.dll' Local Stack Overflow (PoC) / Denial of Service |
windows/dos/53[01;31m[K21[m[K.txt

Visual Events Calendar 1.1 - 'cfg_dir' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K41.txt

Visual Mining NetCharts Server - Remote Code Execution (Metasploit)
| java/remote/35[01;31m[K21[m[K1.rb

Vite 6.2.2 - Arbitrary File Read
| multiple/remote/5[01;31m[K21[m[K11.py

Vlbook 1.[01;31m[K21[m[K - Cross-Site Scripting / Local File Inclusion
| php/webapps/5529.txt

VMware 5.5.1 - COM Object Arbitrary Partition Table Delete
| windows/dos/[01;31m[K21[m[K95.html

VMware GSX Server 2.0 - Authentication Server Buffer Overflow
| windows/remote/[01;31m[K21[m[K639.c

VMware Remote Console e.x.p build-158248 - Format String
| multiple/dos/1[01;31m[K21[m[K88.txt

VMware vSphere Data Protection 5.x/6.x - Java Deserialization
| multiple/remote/4[01;31m[K21[m[K52.py

VMware Workstation 12 Pro - Denial of Service
| windows/dos/4[01;31m[K21[m[K40.c

Volition Red Faction 1.0/1.1 - Game Server/Client Denial of Service
| windows/dos/[01;31m[K21[m[K170.txt

vOlk Botnet Framework 4.0 - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K891.txt

Voodoo chat 1.0RC1b - 'file_path' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K02.txt

Voxel Dot Net CBms 0.x - Multiple Code Injection Vulnerabilities
| php/webapps/[01;31m[K21[m[K517.txt

vqServer 1.9.x - CGI Demo Program Script Injection
| cgi/webapps/[01;31m[K21[m[K411.txt

vSignup 2.1 - SQL Injection
| php/webapps/2[01;31m[K21[m[K68.txt

vTiger CRM 5.4.0/6.0 RC/6.0.0 GA - 'browse.php' Local File Inclusion
| php/webapps/32[01;31m[K21[m[K3.txt

VWar 1.50 R14 - 'online.php' SQL Injection
| php/webapps/[01;31m[K21[m[K70.txt

VX Search Enterprise 9.7.18 - Local Buffer Overflow
| windows/local/4[01;31m[K21[m[K81.py

W-Agora 4.1.6 - 'EditForm.php' Cross-Site Scripting
| php/webapps/2[01;31m[K21[m[K09.txt

W-Agora 4.1.6 - 'index.php?bn' Traversal Arbitrary File Access
| php/webapps/2[01;31m[K21[m[K49.txt

W-Agora 4.1.6 - 'modules.php?File' Traversal Arbitrary File Access
| php/webapps/2[01;31m[K21[m[K50.txt

W-Agora 4.1.x - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K529.txt

W3C Amaya 10.1 Web Browser - 'id' Remote Stack Overflow (PoC)
| windows/dos/7[01;31m[K21[m[K3.pl

W3C CERN HTTPd 3.0 Proxy - Cross-Site Scripting
| unix/remote/[01;31m[K21[m[K704.txt

WAGO 750-8[01;31m[K21[m[K2 PFC200 G2 2ETH RS - Privilege Escalation
| hardware/remote/50793.txt

waldronmatt FullCalendar-BS4-PHP-MySQL-JSON 1.[01;31m[K21[m[K -
'description' Cross-Site Scripting |
php/webapps/47548.txt

waldronmatt FullCalendar-BS4-PHP-MySQL-JSON 1.[01;31m[K21[m[K - 'start'
SQL Injection | php/webapps/47546.txt

WAN Emulator 2.3 - Command Execution (Metasploit)
| linux/remote/[01;31m[K21[m[K190.rb

WAP Proof 2008 - Denial of Service
| windows/dos/[01;31m[K21[m[K147.txt

Watcharr 1.43.0 - Remote Code Execution (RCE)
| multiple/webapps/5[01;31m[K21[m[K30.py

Wav Player 1.1.3.6 - '.pll' Local Buffer Overflow
| windows/local/178[01;31m[K21[m[K.py

WBCE CMS 1.6.3 - Authenticated Remote Code Execution (RCE)
| multiple/webapps/5[01;31m[K21[m[K32.sh

Web Chat Manager 2.0 - HTML Code Injection
| php/webapps/224[01;31m[K21[m[K.txt

Web Help Desk by SolarWinds - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K809.txt

Web Wiz Forum 9.5 - 'admin_category_details.asp?mode' Cross-Site
Scripting |
asp/webapps/3[01;31m[K21[m[K20.txt

Web Wiz Forum 9.5 - 'admin_group_details.asp?mode' Cross-Site Scripting
| asp/webapps/3[01;31m[K21[m[K19.txt

Web Wiz Forums 7.x - 'Registration_Rules.asp' Cross-Site Scripting
| asp/webapps/24[01;31m[K21[m[K4.txt

```
Web Wiz Guestbook 8.[01;31m[K21[m[K - Database Disclosure
| asp/webapps/7488.txt

Web2py 2.14.5 - Multiple Vulnerabilities
| python/webapps/398[01;31m[K21[m[K.txt

WebcamXP 5.3.2.375 - Remote File Disclosure
| windows/remote/75[01;31m[K21[m[K.txt

webERP 4.08.4 - 'WorkOrderEntry.php' SQL Injection
| php/webapps/[01;31m[K21[m[K327.txt

WebFileSys 2.31.0 - Directory Path Traversal
| multiple/webapps/5[01;31m[K21[m[K85.txt

Webify Blog - Arbitrary File Deletion
| php/webapps/[01;31m[K21[m[K250.txt

Webify Business Directory - Arbitrary File Deletion
| php/webapps/[01;31m[K21[m[K270.txt

Webify eDownloads Cart - Arbitrary File Deletion
| php/webapps/[01;31m[K21[m[K269.txt

Webify Photo Gallery - Arbitrary File Deletion
| php/webapps/[01;31m[K21[m[K271.txt

WEBInsta CMS 0.3.1 - 'templates_dir' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K75.py

WEBInsta CMS 0.3.1 - 'users.php' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K89.txt

WEBInsta MM 1.3e - 'absolute_path' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K87.html

WEBInsta MM 1.3e - 'cabsolute_path' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K71.txt

WebKit - 'CachedFrameBase::restore' Universal Cross-Site Scripting
| multiple/webapps/4[01;31m[K21[m[K06.html

WebKit - 'Document::prepareForDestruction' / 'CachedFrame' Universal
Cross-Site Scripting                  |
multiple/webapps/4[01;31m[K21[m[K07.html

WebKit - 'Element::setAttributeNodeNS' Use-After-Free
| multiple/dos/4[01;31m[K21[m[K08.html

WebKit - CachedFrame does not Detach Openers Universal Cross-Site
Scripting                                |
multiple/webapps/4[01;31m[K21[m[K05.html
```

WebKit JSC - 'Intl.getCanonicalLocales' Heap Buffer Overflow
| multiple/dos/4[01;31m[K21[m[K91.html

WebKit JSC - 'JSObject::ensureLength' ensureLengthSlow Check Failure
| linux/dos/4[01;31m[K21[m[K03.js

WebKit JSC - arrayProtoFuncSplice does not Initialize all Indices
| multiple/dos/4[01;31m[K21[m[K89.html

WebKit JSC - Incorrect Check in
emitPutDerivedConstructorToArrowFunctionContextScope
| multiple/dos/4[01;31m[K21[m[K04.js

WebKit JSC - JIT Optimization Check Failed in
IntegerCheckCombiningPhase::handleBlock |
multiple/dos/4[01;31m[K21[m[K90.html

WebKit JSC - JSGlobalObject::haveABadTime Causes Type Confusions
| multiple/dos/4[01;31m[K21[m[K88.html

WebKitGTK+ < 2.[01;31m[K21[m[K.3 - 'WebKitFaviconDatabase' Denial of
Service (Metasploit) | linux/dos/44876.rb

WebKitGTK+ < 2.[01;31m[K21[m[K.3 - Crash (PoC)
| linux/local/44842.txt

WebmasterSite (Multiple Products) - Remote Command Execution
| php/webapps/3[01;31m[K21[m[K88.txt

webmin 0.91 - Directory Traversal
| cgi/remote/[01;31m[K21[m[K183.txt

Webmin 0.x - 'RPC' Privilege Escalation
| linux/remote/[01;31m[K21[m[K765.pl

Webmin 0.x - Code Input Validation
| linux/local/[01;31m[K21[m[K348.txt

Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)
| unix/remote/[01;31m[K21[m[K851.rb

Webmin Usermin 2.100 - Username Enumeration
| perl/webapps/5[01;31m[K21[m[K14.py

WebRTC - VP8 Block Decoding Use-After-Free
| multiple/dos/451[01;31m[K21[m[K.txt

WebScripts WebBBS 4.x/5.0 - Remote Command Execution
| cgi/webapps/[01;31m[K21[m[K567.pl

WebStudio CMS - Blind SQL Injection
| php/webapps/7[01;31m[K21[m[K6.txt

WebTrends Reporting Center for Windows 4.0 d - GET Buffer Overflow
| windows/dos/[01;31m[K21[m[K387.txt

WebTV for Windows 98/ME - Denial of Service
| windows/dos/20[01;31m[K21[m[K9.txt

WebUI 1.5b6 - Remote Code Execution
| php/webapps/368[01;31m[K21[m[K.txt

WEMS BEMS [01;31m[K21[m[K.3.1 - Undocumented Backdoor Account
| hardware/webapps/47817.txt

Western Digital My Cloud 04.01.03-4[01;31m[K21[m[K/04.01.04-422 -
Command Injection |
hardware/webapps/38350.txt

WFTPD Pro Server 3.[01;31m[K21[m[K - MLST Remote Denial of Service
| windows/dos/427.c

WFTPD Server 3.[01;31m[K21[m[K - Remote Buffer Overflow
| windows/remote/159.c

WFTPD Server GUI 3.[01;31m[K21[m[K - Remote Denial of Service
| windows/dos/23842.pl

Whatsapp 2.19.[01;31m[K21[m[K6 - Remote Code Execution
| android/remote/47515.cpp

WhatsUpGold [01;31m[K21[m[K.0.3 - Stored Cross-Site Scripting (XSS)
| multiple/webapps/50366.txt

Wheatblog 1.1 - 'session.php' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K74.txt

WhitSoft Development SlimFTPd 3.17 - Remote Denial of Service
| windows/dos/26[01;31m[K21[m[K9.c

WiFi HD 8.1 - Directory Traversal / Denial of Service
| ios/webapps/37[01;31m[K21[m[K3.txt

WikiWebHelp 0.28 - SQL Injection
| php/webapps/14[01;31m[K21[m[K7.txt

WikkiTikkiTavi 0.x - Remote File Inclusion
| php/webapps/[01;31m[K21[m[K241.txt

William Deich Super 3.x - SysLog Format String
| linux/local/[01;31m[K21[m[K674.c

Willoughby TriO 2.1 - SQL Injection
| php/webapps/3[01;31m[K21[m[K17.txt

```
Winamp - MAKI Buffer Overflow (Metasploit)
| windows/local/[01;31m[K21[m[K256.rb

Winamp 5.[01;31m[K21[m[K - '.Midi' File Header Handling Buffer Overflow
(PoC)                                          | windows/dos/1935.cpp

Windows 10 v[01;31m[K21[m[KH1 - HTTP Protocol Stack Remote Code
Execution                                                  |
windows/remote/51575.txt

Windscribe - WindscribeService Named Pipe Privilege Escalation
(Metasploit)                                |
windows/local/480[01;31m[K21[m[K.rb

WinduCMS 3.1 - Local File Disclosure
| php/webapps/43[01;31m[K21[m[K4.py

Wing FTP Server 3.2.4 - Cross-Site Request Forgery
| multiple/webapps/108[01;31m[K21[m[K.txt

WinIPDS 3.3 rev. G52-33-0[01;31m[K21[m[K - Directory Traversal / Denial
of Service                                     |
windows/remote/31163.txt

WINMOD 1.4 - '.lst' Local Buffer Overflow (SEH)
| windows/local/92[01;31m[K21[m[K.pl

WinRAR 2.90/3.0/3.10 - Archive File Extension Buffer Overrun
| windows/local/2[01;31m[K21[m[K93.txt

WinRar 5.[01;31m[K21[m[K - SFX OLE Command Execution
| windows/local/38319.py

WinSyslog Interactive Syslog Server 4.[01;31m[K21[m[K - long Message
Remote Denial of Service                       |
windows/dos/23242.pl

Wireless Tools 26 (IWConfig) - Local Privilege Escalation
| linux/local/1[01;31m[K21[m[K5.c

Wireshark 1.2.10 - 'airpcap.dll' DLL Hijacking
| windows/local/147[01;31m[K21[m[K.c

Wireshark 2.2.0 < 2.2.12 - ROS Dissector Denial of Service
| multiple/dos/4[01;31m[K21[m[K24.txt

Wireshark 2.2.6 - IPv6 Dissector Denial of Service
| multiple/dos/4[01;31m[K21[m[K23.txt

WMMon 1.0 b2 - Memory Character File Open File Descriptor Read
| freebsd/local/[01;31m[K21[m[K798.txt
```

WMNet2 1.0 6 - Kernel Memory File Descriptor Leakage
| freebsd/local/[01;31m[K21[m[K799.txt

WMV to AVI MPEG DVD WMV Convertor 4.6.1[01;31m[K21[m[K7 - Buffer
OverFlow (SEH) |
windows/local/47568.py

WMV to AVI MPEG DVD WMV Convertor 4.6.1[01;31m[K21[m[K7 - Denial of
Service |
windows/dos/47563.py

Wolf CMS 0.8.3.1 - Remote Code Execution (RCE)
| php/webapps/514[01;31m[K21[m[K.txt

WolfCMS 0.8.3.1 - Open Redirection
| php/webapps/444[01;31m[K21[m[K.txt

Wolfram Research webMathematica 4.0 - File Disclosure
| java/webapps/[01;31m[K21[m[K562.txt

WoltLab Burning Board 2.0 - SQL Injection
| php/webapps/[01;31m[K21[m[K779.txt

Wondershare Driver Install Service help 10.7.1.3[01;31m[K21[m[K -
'ElevationService' Unquote Service Path |
windows/local/49101.txt

WordPress Core 0.6/0.7 - 'Blog.header.php' SQL Injection
| php/webapps/23[01;31m[K21[m[K3.txt

WordPress Core 2.3.1 - Charset SQL Injection
| php/webapps/47[01;31m[K21[m[K.txt

WordPress Core 2.6.1 - Admin Takeover (SQL Column Truncation)
| php/webapps/64[01;31m[K21[m[K.php

WordPress Plugin / Joomla! Component XCloner - Multiple Vulnerabilities
| php/webapps/35[01;31m[K21[m[K2.txt

Wordpress Plugin 3dady real-time web stats 1.0 - Stored Cross Site
Scripting (XSS) |
php/webapps/510[01;31m[K21[m[K.txt

Wordpress Plugin 3DPrint Lite 1.9.1.4 - Arbitrary File Upload
| php/webapps/503[01;31m[K21[m[K.py

WordPress Plugin Adminimize 1.7.[01;31m[K21[m[K - 'page' Cross-Site
Scripting |
php/webapps/36325.txt

WordPress Plugin Blue Admin [01;31m[K21[m[K.06.01 - Cross-Site Request
Forgery (CSRF) |
php/webapps/50925.html

WordPress Plugin Bulk Delete 5.5.3 - Privilege Escalation
| php/webapps/395[01;31m[K21[m[K.txt

WordPress Plugin Chained Quiz 1.0.8 - 'answer' SQL Injection
| php/webapps/452[01;31m[K21[m[K.txt

WordPress Plugin Comment Rating 2.9.23 - Multiple Vulnerabilities
| php/webapps/162[01;31m[K21[m[K.txt

WordPress Plugin Custom Searchable Data System - Unauthenticated Data
M]odification |
php/webapps/48[01;31m[K21[m[K3.txt

WordPress Plugin Event List < 0.7.8 - SQL Injection
| php/webapps/4[01;31m[K21[m[K73.txt

WordPress Plugin Featured Comments - Cross-Site Request Forgery
| php/webapps/39[01;31m[K21[m[K3.txt

WordPress Plugin IMDb Profile Widget 1.0.8 - Local File Inclusion
| php/webapps/396[01;31m[K21[m[K.txt

WordPress Plugin JoomSport 3.3 - SQL Injection
| php/webapps/47[01;31m[K21[m[K0.txt

WordPress Plugin JW Player for Flash & HTML5 Video - Cross-Site Request
Forgery | php/webapps/39[01;31m[K21[m[K2.txt

WordPress Plugin LifterLMS 4.[01;31m[K21[m[K.0 - Stored Cross-Site
Scripting (XSS) |
php/webapps/49912.txt

WordPress Plugin Product Slider for WooCommerce 1.13.[01;31m[K21[m[K -
Cross Site Scripting (XSS) |
php/webapps/50704.txt

WordPress Plugin Realty - Blind SQL Injection
| php/webapps/290[01;31m[K21[m[K.txt

WordPress Plugin ReDi Restaurant Reservation [01;31m[K21[m[K.0307 -
'Comment' Stored Cross-Site Scripting (XSS) |
php/webapps/49903.txt

WordPress Plugin SermonBrowser 0.43 - SQL Injection
| php/webapps/17[01;31m[K21[m[K4.php

Wordpress Plugin Simple Job Board 2.9.3 - Local File Inclusion
| php/webapps/507[01;31m[K21[m[K.py

WordPress Plugin social discussions 6.1.1 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K21[m[K58.txt

Wordpress Plugin SP Project & Document Manager 4.[01;31m[K21[m[K -
Remote Code Execution (RCE) (Authenticated) |
php/webapps/50115.py

WordPress Plugin spider Calendar - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K715.txt

WordPress Plugin Stop Spammers 20[01;31m[K21[m[K.8 - 'log' Reflected
Cross-site Scripting (XSS) |
php/webapps/49880.txt

WordPress Plugin SupportEzzy Ticket System 1.2.5 - Persistent Cross-
Site Scripting |
php/webapps/35[01;31m[K21[m[K8.txt

WordPress Plugin Thinkun Remind 1.1.3 - Remote File Disclosure
| php/webapps/190[01;31m[K21[m[K.txt

WordPress Plugin Time Capsule 1.[01;31m[K21[m[K.16 - Authentication
Bypass |
php/webapps/47941.py

WordPress Plugin Tribulant Newsletters 4.6.4.2 - File Disclosure /
Cross-Site Scripting |
php/webapps/4[01;31m[K21[m[K29.txt

WordPress Plugin User Role Editor 3.12 - Cross-Site Request Forgery
| php/webapps/257[01;31m[K21[m[K.txt

WordPress Plugin UserPro < 4.9.[01;31m[K21[m[K - User Registration
Privilege Escalation |
php/webapps/46083.txt

WordPress Plugin White Label CMS 1.5 - Cross-Site Request Forgery /
Persistent Cross-Site Scripting |
php/webapps/2[01;31m[K21[m[K56.txt

WordPress Plugin WooCommerce Store Toolkit 1.5.5 - Privilege Escalation
| php/webapps/394[01;31m[K21[m[K.py

WordPress Plugin Wow Viral Signups 2.1 - SQL Injection
| php/webapps/419[01;31m[K21[m[K.txt

WordPress Plugin WP Jobs < 1.5 - SQL Injection
| php/webapps/4[01;31m[K21[m[K72.txt

WordPress Plugin WP Prayer version 1.6.1 - 'prayer_messages' Stored
Cross-Site Scripting (XSS) (Authentica |
php/webapps/499[01;31m[K21[m[K.txt

WordPress Plugin WP Symposium Pro 20[01;31m[K21[m[K.10 -
'wps_admin_forum_add_name' Stored Cross-Site Scripting (XSS) |
php/webapps/50514.txt

```
WordPress Plugin wp-gpx-map 1.1.[01;31m[K21[m[K - Arbitrary File Upload
| php/webapps/19050.txt

WordPress Plugin WP-Testimonials < 3.4.1 - SQL Injection
| php/webapps/4[01;31m[K21[m[K66.txt

WordPress Plugin wp-topbar 4.02 - Multiple Vulnerabilities
| php/webapps/[01;31m[K21[m[K393.txt

WordPress Plugin Xorbin Digital Flash Clock - 'widgetUrl' Cross-Site
Scripting                              |
php/webapps/386[01;31m[K21[m[K.txt

WordPress Plugin Z-Vote 1.1 - SQL Injection
| php/webapps/16[01;31m[K21[m[K8.txt

WordPress Theme Archin 3.2 - Configuration Access
| php/webapps/[01;31m[K21[m[K646.py

WordPress Theme Curvo - Cross-Site Request Forgery / Arbitrary File
Upload                                  |
php/webapps/29[01;31m[K21[m[K1.txt

WordPress Theme Infocus - '/infocus/lib/scripts/dl-skin.php' Local File
Disclosure                          | php/webapps/39[01;31m[K21[m[K1.txt

WordPress User Registration & Membership Plugin 4.1.1 - Unauthenticated
Privilege Escalation                |
multiple/webapps/5[01;31m[K21[m[K37.txt

WorkforceROI Xpede 4.1/7.0 - Weak Password Encryption
| windows/local/[01;31m[K21[m[K351.pl

Working Resources 1.7.3 BadBlue - Null Byte File Disclosure
| windows/remote/[01;31m[K21[m[K616.txt

Working Resources 1.7.x BadBlue - Administrative Interface Arbitrary
File Access                             |
windows/remote/[01;31m[K21[m[K630.html

Working Resources BadBlue 1.5/1.6 - Directory Traversal
| windows/remote/[01;31m[K21[m[K303.txt

Working Resources BadBlue 1.7 - 'ext.dll' Cross-Site Scripting
| windows/remote/[01;31m[K21[m[K576.txt

Working Resources BadBlue 1.7.3 - 'cleanSearchString()' Cross-Site
Scripting                               |
windows/remote/[01;31m[K21[m[K599.txt

Working Resources BadBlue 1.7.3 - GET Denial of Service
| windows/dos/[01;31m[K21[m[K600.txt
```

WorldClient 5.0.x - Arbitrary File Deletion
| windows/remote/[01;31m[K21[m[K438.txt

WorldSpan Res Manager 4.1 - Malformed TCP Packet Denial of Service
| windows/dos/[01;31m[K21[m[K594.pl

Worldviewer.com CMS - SQL Injection
| php/webapps/1[01;31m[K21[m[K63.txt

WoW Roster 1.70 - '/lib/phpBB.php' Remote File Inclusion
| php/webapps/[01;31m[K21[m[K09.txt

WOW[01;31m[K21[m[K 5.0.1.9 - 'Service WOW[01;31m[K21[m[K_Service'
Unquoted Service Path |
windows/local/50818.txt

Wrapper.php for osCommerce - Local File Inclusion
| php/webapps/30[01;31m[K21[m[K7.txt

WSN Forum 1.[01;31m[K21[m[K - 'memberlist.php' SQL Injection
| php/webapps/26567.txt

WSN Guest 1.[01;31m[K21[m[K - 'id' SQL Injection
| php/webapps/3477.html

WU-FTPD 2.6 - File Globbing Heap Corruption
| unix/remote/[01;31m[K21[m[K161.txt

WU-IMAPd 2000/2001 - Partial Mailbox Attribute Remote Buffer Overflow
(1) |
linux/remote/[01;31m[K21[m[K442.c

WU-IMAPd 2000/2001 - Partial Mailbox Attribute Remote Buffer Overflow
(2) |
linux/remote/[01;31m[K21[m[K443.c

wwwstats 3.[01;31m[K21[m[K - 'Clickstats.php' Multiple HTML Injection
Vulnerabilities |
php/webapps/30854.sh

X Window 4.0/4.1/4.2 - System Oversized Font Denial of Service
| linux/dos/[01;31m[K21[m[K518.txt

X-Chat 1.x - CTCP Ping Remote IRC Command Execution
| linux/remote/[01;31m[K21[m[K[01;31m[K21[m[K0.txt

x10 mirco blogging 1[01;31m[K21[m[K - SQL Injection
| php/webapps/12042.txt

X2Engine 4.2 - Cross-Site Request Forgery
| php/webapps/383[01;31m[K21[m[K.txt

XAMPP 3.2.1 & phpMyAdmin 4.1.6 - Multiple Vulnerabilities
| php/webapps/327[01;31m[K21[m[K.txt

XAMPP Linux 1.6 - 'iart.php?text' Cross-Site Scripting
| linux/remote/3[01;31m[K21[m[K66.txt

XAMPP Linux 1.6 - 'ming.php?text' Cross-Site Scripting
| linux/remote/3[01;31m[K21[m[K65.txt

Xavier 2.4 - SQL Injection
| php/webapps/4[01;31m[K21[m[K32.txt

xBtiTracker - SQL Injection
| php/webapps/1[01;31m[K21[m[K40.php

XChat 2.6.7 (Windows) - Remote Denial of Service
| windows/dos/[01;31m[K21[m[K24.php

XChat 2.6.7 (Windows) - Remote Denial of Service
| windows/dos/[01;31m[K21[m[K47.pl

Xerver 2.10 - Multiple Request Denial of Service Vulnerabilities
| windows/dos/[01;31m[K21[m[K336.txt

XFree86 4.2 - 'XLOCALEDIR' Local Buffer Overflow (2)
| linux/local/223[01;31m[K21[m[K.c

XFree86 X11R6 3.3.2 XMan - ManPath Environment Variable Buffer Overflow
| linux/local/[01;31m[K21[m[K010.sh

XGB 1.2 - Remote Form Field Input Validation
| php/webapps/[01;31m[K21[m[K382.txt

XGB Guestbook 1.2 - User-Embedded Scripting
| php/webapps/[01;31m[K21[m[K381.txt

Xinet Elegant 6 Asset Lib Web UI 6.1.655 - SQL Injection
| multiple/webapps/5[01;31m[K21[m[K92.py

Xion Audio Player 1.0 1[01;31m[K21[m[K - '.m3u' Local Buffer Overflow
(2) |
windows/local/9983.pl

Xion Audio Player 1.0 1[01;31m[K21[m[K - '.m3u' Remote Buffer Overflow
(1) |
windows/remote/9851.pl

XM Easy Personal FTP Server 5.8.0 - Remote Denial of Service
| windows/dos/102[01;31m[K21[m[K.txt

XMail 1.[01;31m[K21[m[K - '-t' Command Line Option Local Buffer
Overflow / Local Privilege Escalation |
linux/local/1267.c

XMB 1.9.6 - 'mq=off' 'u2uid' SQL Injection
| php/webapps/[01;31m[K21[m[K05.php

XMB 1.9.6 Final - 'basename()' Remote Command Execution
| php/webapps/[01;31m[K21[m[K78.php

XMB Forum 1.6 - Magic Lantern Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K447.txt

XMB Forum 1.6 - Magic Lantern Log File
| php/webapps/[01;31m[K21[m[K448.txt

XMB Forum 1.6 pre-beta - Image Tag Script Injection
| php/webapps/[01;31m[K21[m[K300.txt

XMB Forum 1.8 - 'buddy.php?action' Cross-Site Scripting
| php/webapps/228[01;31m[K21[m[K.txt

XMB Forum 1.8 - 'member.php' SQL Injection
| php/webapps/225[01;31m[K21[m[K.c

XMPlay 3.3.0.4 - '.PLS' Local Buffer Overflow
| windows/local/28[01;31m[K21[m[K.c

xNews 1.3 - 'xNews.php' SQL Injection
| php/webapps/3[01;31m[K21[m[K6.txt

xNewsletter 1.0 - Form Field Input Validation
| php/webapps/[01;31m[K21[m[K383.txt

XnView 1.98 - Denial of Service (PoC)
| windows/dos/174[01;31m[K21[m[K.py

XnView 1.99.1 - '.JLS' File Decompression Heap Overflow
| windows/dos/[01;31m[K21[m[K741.txt

Xomol CMS 1.2 - '/index.php' HTML Injection / Cross-Site Scripting
| php/webapps/320[01;31m[K21[m[K.txt

XOOPS 1.0 RC3 - HTML Injection
| php/webapps/[01;31m[K21[m[K829.txt

XOOPS Module Glossario 2.2 - 'sid' SQL Injection
| php/webapps/5[01;31m[K21[m[K6.txt

XOOPS Module resmanager 1.[01;31m[K21[m[K - Blind SQL Injection
| php/webapps/3931.html

XOOPS Module Tutoriais - 'viewcat.php' SQL Injection
| php/webapps/36[01;31m[K21[m[K.pl

XOOPS Module wfdownloads - 'cid' SQL Injection
| php/webapps/5[01;31m[K21[m[K8.txt

XP Book 3.0 - login Admin
| php/webapps/106[01;31m[K21[m[K.txt

XRms 1.99.2 - 'company_name' Cross-Site Scripting
| php/webapps/323[01;31m[K21[m[K.txt

Xserver 0.1 Alpha - 'POST' Remote Buffer Overflow (PoC)
| linux/dos/4[01;31m[K21[m[K6.pl

xtell 1.91.1/2.6.1 - Multiple Remote Buffer Overflow Vulnerabilities
| linux/remote/[01;31m[K21[m[K309.c

xtell 2.6.1 - User Status Remote Information Disclosure
| linux/remote/[01;31m[K21[m[K310.txt

XTux Server 2001.0 6.01 - Garbage Denial of Service
| linux/dos/[01;31m[K21[m[K338.pl

xWeblog 2.2 - 'arsiv.asp?tarih' SQL Injection
| asp/webapps/15[01;31m[K21[m[K9.py

xWeblog 2.2 - 'oku.asp?makale_id' SQL Injection
| asp/webapps/15[01;31m[K21[m[K8.txt

XWiki Platform 15.10.10 - Remote Code Execution
| multiple/webapps/5[01;31m[K21[m[K36.txt

XWiki Standard 14.10 - Remote Code Execution (RCE)
| php/webapps/5[01;31m[K21[m[K05.py

Xynph FTP Server 1.0 - Directory Traversal
| windows/remote/2[01;31m[K21[m[K44.txt

YaBB 1 - Invalid Topic Error Page Cross-Site Scripting
| cgi/webapps/[01;31m[K21[m[K573.txt

YABB 1.4.1 SE - 'Reminder.php' SQL Injection
| php/webapps/2[01;31m[K21[m[K46.txt

YaBB 1.40/1.41 - Login Cross-Site Scripting
| php/webapps/[01;31m[K21[m[K950.txt

YaBB 9.1.2000 - Arbitrary File Read
| cgi/remote/20[01;31m[K21[m[K8.txt

YaBB 9.1.2000 - Cross-Agent Scripting
| cgi/webapps/[01;31m[K21[m[K208.txt

YABB SE 0.8/1.4/1.5 - 'Packages.php' Remote File Inclusion
| php/webapps/2[01;31m[K21[m[K92.pl

Yahoo! Messenger 5.0 - Call Center Buffer Overflow
| windows/remote/[01;31m[K21[m[K484.c

Yahoo! Messenger 8.1.0.4[01;31m[K21[m[K - CYFT Object Arbitrary File Download |
windows/remote/4428.html

Yahoo! Messenger 9.0.0.[01;31m[K21[m[K62 - 'YahooBridgeLib.dll' ActiveX Control Remote Denial of Service | windows/dos/10092.txt

YAP 1.1.1 - Blind SQL Injection / SQL Injection
| php/webapps/8[01;31m[K21[m[K7.txt

YaPiG 0.94.0u - Remote File Inclusion
| php/webapps/1[01;31m[K21[m[K64.txt

Yellow Swordfish Simple Forum 1.10/1.11 - 'topic' SQL Injection
| php/webapps/31[01;31m[K21[m[K0.txt

Yellow Swordfish Simple Forum 1.7/1.9 - 'index.php' SQL Injection
| php/webapps/31[01;31m[K21[m[K1.txt

Yellow Swordfish Simple Forum 1.x - 'topic' SQL Injection
| php/webapps/31[01;31m[K21[m[K2.txt

YenerTurk Haber Script 1.0 - SQL Injection
| asp/webapps/[01;31m[K21[m[K38.txt

YepYep MTFTPD 0.2/0.3 - Remote CWD Argument Format String
| linux/remote/253[01;31m[K21[m[K.c

YesWiki 4.5.1 - Unauthenticated Path Traversal
| multiple/webapps/5[01;31m[K21[m[K35.txt

Yogurt Social Network 3.2 rc1 Module for XOOPS - 'friends.php?uid' Cross-Site Scripting |
php/webapps/3[01;31m[K21[m[K98.txt

Yogurt Social Network 3.2 rc1 Module for XOOPS - 'seutubo.php?uid' Cross-Site Scripting |
php/webapps/3[01;31m[K21[m[K99.txt

Yokogawa CENTUM CS 3000 - 'BKBCopyD.exe' Remote Buffer Overflow (Metasploit) |
windows/remote/32[01;31m[K21[m[K0.rb

Youngzsoft CMailServer 3.30/4.0 - Remote Buffer Overflow (1)
| windows/remote/[01;31m[K21[m[K466.c

Youngzsoft CMailServer 3.30/4.0 - Remote Buffer Overflow (2)
| windows/remote/[01;31m[K21[m[K467.c

Yourownbux 3.1/3.2 Beta - SQL Injection
| php/webapps/63[01;31m[K21[m[K.txt

```
Zabbix - (Authenticated) Remote Command Execution (Metasploit)
| linux/remote/293[01;31m[K21[m[K.rb

ZDaemon 1.8 - Null Pointer Remote Denial of Service
| multiple/dos/3[01;31m[K21[m[K04.txt

ZEN Load Balancer Filelog - Command Execution (Metasploit)
| unix/remote/[01;31m[K21[m[K849.rb

Zend-Framework - Full Information Disclosure
| php/webapps/299[01;31m[K21[m[K.py

Zenoss Monitoring System 4.2.5-[01;31m[K21[m[K08 (x64) - Persistent
Cross-Site Scripting                                    |
multiple/webapps/34165.txt

Zenturi NixonMyPrograms Class 'sasatl.dll 1.5.0.531' - Remote Buffer
Overflow                                |
windows/remote/4[01;31m[K21[m[K4.html

Zenturi ProgramChecker - ActiveX 'sasatl.dll' Remote Buffer Overflow
| windows/remote/40[01;31m[K21[m[K.html

ZeroBoard 4.1 - PHP Include File Arbitrary Command Execution
| php/webapps/[01;31m[K21[m[K557.txt

Zervit Web Server 0.04 - GET Remote Buffer Overflow (PoC)
| windows/dos/87[01;31m[K21[m[K.pl

Zikula Application Framework 1.2.7/1.3 - 'themename' Cross-Site
Scripting                                  |
php/webapps/361[01;31m[K21[m[K.txt

zkfingerd 0.9.1 - 'say()' Format String
| linux/remote/2[01;31m[K21[m[K01.c

zKup CMS 2.0 < 2.3 - Remote Add Admin
| php/webapps/5[01;31m[K21[m[K9.php

ZOHO ManageEngine ADSelfService Plus 4.5 Build 45[01;31m[K21[m[K -
Cross-Site Scripting                                    |
php/webapps/36316.txt

Zohocorp ManageEngine ADManager Plus 7[01;31m[K21[m[K0 - Elevation of
Privilege                                               |
multiple/webapps/5[01;31m[K21[m[K48.txt

Zone Labs ZoneAlarm 3.0/3.1 - Syn Flood Denial of Service
| windows/dos/[01;31m[K21[m[K943.c

ZoneAlarm Pro 1.0/2.x - Outbound Packet Bypass
| windows/remote/[01;31m[K21[m[K169.txt
```

ZoneX 1.0.3 - Publishers Gold Edition Remote File Inclusion
| php/webapps/[01;31m[K21[m[K42.txt

Zoom VoIP Phone Adapater ATA1+1 1.2.5 - Cross-Site Request Forgery
| hardware/remote/79[01;31m[K21[m[K.txt

Zope 2.x - Incorrect XML-RPC Request Information Disclosure
| linux/remote/[01;31m[K21[m[K870.txt

Zortam Mp3 Media Studio [01;31m[K21[m[K.15 - Insecure File Permissions
Privilege Escalation |
windows/local/40418.txt

ZTE PC UI USB Modem Software - Local Buffer Overflow
| windows/local/38[01;31m[K21[m[K9.py

ZTE ZXHN H168N 3.1 - Remote Code Execution (RCE) via authentication
bypass |
multiple/hardware/5[01;31m[K21[m[K91.py

ZYXEL Prestige 642R Router - Malformed IP Packet Denial of Service
| hardware/dos/[01;31m[K21[m[K637.c

ZYXEL Prestige 642R Router - Malformed Packet Denial of Service
| hardware/dos/[01;31m[K21[m[K561.txt

ZYXEL Prestige 681 SDSL Router - IP Fragment Reassembly
| hardware/remote/[01;31m[K21[m[K186.txt

Zyxel USG FLEX 5.[01;31m[K21[m[K - OS Command
Injection
| hardware/remote/50946.txt

Shellcode Title
| Path

Cisco IOS - New TTY + Privilege Level To 15 + Reverse
([01;31m[K21[m[K/TCP) Virtual Terminal Shell Shellcode |
hardware/13291.asm

Linux - setreuid(0_0) + execve(_/bin/sh__NULL_NULL) + XOR Encoded
Shellcode (62 bytes) | linux/14[01;31m[K21[m[K9.c

Linux - Write SUID Root Shell (/tmp/.hiddenshell) + Polymorphic
Shellcode (161 bytes) | linux/14[01;31m[K21[m[K8.c

Linux/ARM (Raspberry Pi) - chmod 0777 /etc/shadow Shellcode (41 bytes)
| arm/[01;31m[K21[m[K254.asm

Linux/ARM (Raspberry Pi) - execve(_/bin/sh__ [0]_ [0 vars]) Shellcode
(30 bytes) | arm/[01;31m[K21[m[K253.asm

Linux/ARM (Raspberry Pi) - Reverse (10.1.1.2:0x1337/TCP) Shell
(/bin/sh) Shellcode (72 bytes) |
arm/[01;31m[K21[m[K252.asm

Linux/ARM - Bind TCP (0.0.0.0:43[01;31m[K21[m[K) Shell (/bin/sh) +
Null-Free Shellcode (84 bytes) | arm/46264.s

Linux/ARM - Reverse (192.168.1.124:43[01;31m[K21[m[K/TCP) Shell
(/bin/sh) Shellcode (64 bytes) | arm/46258.s

Linux/ARM - Reverse (192.168.1.1:4444/TCP) Shell (/bin/sh)+ Null-Free
Shellcode (80 bytes) | arm/439[01;31m[K21[m[K.asm

Linux/SPARC - Reverse (192.168.100.1:2313/TCP) Shell Shellcode
([01;31m[K21[m[K6 bytes) |
linux_sparc/13305.c

Linux/x64 - execve(/bin/sh) Shellcode ([01;31m[K21[m[K bytes)
| linux_x86-64/41750.asm

Linux/x64 - execve(/bin/sh) Shellcode ([01;31m[K21[m[K bytes) (2)
| linux_x86-64/49770.c

Linux/x64 - execve(/bin/sh) Shellcode (24 bytes)
| linux_x86-64/4[01;31m[K21[m[K79.c

Linux/x64 - execve(/bin/sh) Shellcode (31 bytes) (1)
| linux_x86-64/4[01;31m[K21[m[K26.c

Linux/x86 - Bind (17771/TCP) Netcat (/bin/nc) Shell (/bin/sh) Shellcode
(58 bytes) | linux_x86/369[01;31m[K21[m[K.c

Linux/x86 - Bind (64533/TCP) Shell (/bin/sh) Shellcode (97 bytes)
| linux_x86/14[01;31m[K21[m[K6.c

Linux/x86 - Bind (99999/TCP) NetCat Traditional (/bin/nc) Shell
(/bin/bash) Shellcode (58 bytes) |
linux_x86/458[01;31m[K21[m[K.c

Linux/x86 - chmod 777 (/etc/passwd + /etc/shadow) + Add Root User
(ALI/ALI) To /etc/passwd + setreuid() + | linux_x86/34592.c

Linux/x86 - execve(/bin/sh) + Null-Free Shellcode ([01;31m[K21[m[K
bytes) (6) |
linux_x86/43735.c

Linux/x86 - execve(/bin/sh) + Push Method Shellcode ([01;31m[K21[m[K bytes) | linux_x86/36857.c

Linux/x86 - execve(/bin/sh) + setuid(0) + setgid(0) + XOR Encoded Shellcode (66 bytes) | linux_x86/4[01;31m[K21[m[K77.c

Linux/x86 - execve(/bin/sh) + Standard Opcode Array Payload Shellcode ([01;31m[K21[m[K bytes) | linux_x86/13409.c

Linux/x86 - execve(/bin/sh) Shellcode (18 bytes) | linux_x86/443[01;31m[K21[m[K.c

Linux/x86 - execve(/bin/sh) Shellcode ([01;31m[K21[m[K bytes) (1) | linux_x86/37251.asm

Linux/x86 - execve(/bin/sh) Shellcode ([01;31m[K21[m[K bytes) (2) | linux_x86/13628.c

Linux/x86 - execve(/bin/sh) Shellcode ([01;31m[K21[m[K bytes) (3) | linux_x86/43702.c

Linux/x86 - execve(/bin/sh) Shellcode ([01;31m[K21[m[K bytes) (4) | linux_x86/41757.txt

Linux/x86 - execve(/bin/sh) Using JMP-CALL-POP Shellcode ([01;31m[K21[m[K bytes) | linux_x86/47068.c

Linux/x86 - execve(/bin/sh_0_0) Shellcode ([01;31m[K21[m[K bytes) | linux_x86/43658.c

Linux/x86 - execve(_/bin/ash__0_0) Shellcode ([01;31m[K21[m[K bytes) | linux_x86/13423.c

Linux/x86 - Flush IPTables Rules (iptables --flush) Shellcode (43 bytes) | linux_x86/437[01;31m[K21[m[K.c

Linux/x86 - Reverse (192.168.3.119:543[01;31m[K21[m[K/TCP) Shell (/bin/bash) Shellcode (110 bytes) | linux_x86/41723.c

Linux/x86 - Reverse (543[01;31m[K21[m[K/UDP) tcpdump Live Packet Capture Shellcode (151 bytes) | linux_x86/13329.c

Linux/x86 - Self-Modifying Magic Byte /bin/sh Shellcode (76 bytes) | linux_x86/134[01;31m[K21[m[K.c

Linux/x86 - Serial Port Shell Binding (/dev/ttyS0) + busybox Launching Null-Free Shellcode (82 bytes) | linux_x86/133[01;31m[K21[m[K.c

OSX/PPC - Add Root User (r00t) Shellcode ([01;31m[K21[m[K9 bytes)
| osx_ppc/13480.c

OSX/PPC / OSX/x86 - execve(_/bin/sh__{_/bin/sh__NULL}_NULL) Shellcode
(1[01;31m[K21[m[K bytes) | multiple/13466.c

Safari 4.0.5 < 5.0.0 (Windows XP/7) - JavaScript JITed exec calc
(ASLR/DEP Bypass) + Null-Free Shellcode |
windows/142[01;31m[K21[m[K.html

Solaris/SPARC - setreuid(geteuid()) + setregid(getegid()) +
execve(/bin/sh) Shellcode |
solaris_sparc/436[01;31m[K21[m[K.c

Windows (XP SP1) - Bind (588[01;31m[K21[m[K/TCP) Shell Shellcode (116
bytes) | windows_x86/13531.c

Windows/x64 - Add Administrator User (ALI/ALI) + Add To RDP Group +
Enable RDP From Registry + Stop Firewa | windows_x86-64/35794.txt

Windows/x64 - Download File (http://192.168.10.129/pl.exe) + Execute
(C:/Users/Public/p.exe) Shellcode (35 | windows_x86-
64/408[01;31m[K21[m[K.c

Windows/x64 - PIC Null-Free TCP Reverse Shell Shellcode (476 Bytes)
| windows/517[01;31m[K21[m[K.py

Windows/x64 - URLDownloadToFileA(http://localhost/trojan.exe) + Execute
Shellcode ([01;31m[K21[m[K8+ bytes) | windows_x86-
64/13533.asm

Windows/x64 - WinExec Add-Admin (ROOT/I@mR00T$) Dynamic Null-Free
Shellcode ([01;31m[K21[m[K0 Bytes) | windows_x86-
64/48252.txt

Windows/x86 (2000) - Reverse (192.168.0.247:87[01;31m[K21[m[K/TCP)
Connect + Vampiric Import Shellcode (179 bytes) |
windows_x86/43760.asm

Windows/x86 (NT/XP/2000/2003) - Bind (87[01;31m[K21[m[K/TCP) Shell
Shellcode (356 bytes) |
windows_x86/43759.asm

Windows/x86 - Add Administrator User (ALI/ALI) + Add To RDP Group +
Enable RDP From Registry + Stop Firewa | windows_x86/35793.txt

Windows/x86 - Command WinExec() Shellcode (104+ bytes)
| windows_x86/135[01;31m[K21[m[K.asm

Windows/x86 - Download File (http://192.168.10.10/evil.exe
c:\evil.exe) Via bitsadmin + Execute Shellc | windows_x86/47041.c

---

Port: 2121

Exploit Title
| Path

Angular-Base64-Upload Library 0.1.20 - Remote Code Execution (RCE)
| multiple/remote/5[01;31m[K2121[m[K.py

BIND 9.10.5 - Unquoted Service Path Privilege Escalation
| windows/local/4[01;31m[K2121[m[K.txt

Cacheflow CacheOS 3.1/4.0 Web Administration - Arbitrary Cached Page Code Leakage |
multiple/remote/[01;31m[K2121[m[K2.txt

CDRDAO 1.1.x - Home Directory Configuration File Symbolic Link (1)
| linux/local/[01;31m[K2121[m[K6.sh

CDRDAO 1.1.x - Home Directory Configuration File Symbolic Link (2)
| linux/local/[01;31m[K2121[m[K7.sh

CDRDAO 1.1.x - Home Directory Configuration File Symbolic Link (3)
| linux/local/[01;31m[K2121[m[K8.sh

CDRDAO 1.1.x - Home Directory Configuration File Symbolic Link (4)
| linux/local/[01;31m[K2121[m[K9.sh

EServ 2.9x - Password-Protected File Access
| windows/remote/[01;31m[K2121[m[K1.txt

EType EServ 2.9x - FTP Remote Denial of Service
| windows/dos/2[01;31m[K2121[m[K.pl

FreeWnn 1.1 0 - jserver JS_MKDIR MetaCharacter Command Execution
| unix/remote/[01;31m[K2121[m[K5.c

Jamroom 3.3.8 - Cookie Authentication Bypass
| php/webapps/3[01;31m[K2121[m[K.php

Joomla! Component JA Voice 2.0 - Local File Inclusion
| php/webapps/1[01;31m[K2121[m[K.txt

SapporoWorks Black JumboDog 2.6.4/2.6.5 - HTTP Proxy Buffer Overflow
| windows/remote/[01;31m[K2121[m[K4.c

Snort 1.8.3 - ICMP Denial of Service
| multiple/dos/[01;31m[K2121[m[K3.txt

Torbstoff News 4 - 'pfad' Remote File Inclusion
| php/webapps/[01;31m[K2121[m[K.txt

X-Chat 1.x - CTCP Ping Remote IRC Command Execution
| linux/remote/[01;31m[K2121[m[K0.txt

Shellcodes: No Results

Port: 22

Exploit Title
| Path

.netCART Settings.XML - Information Disclosure
| asp/webapps/[01;31m[K22[m[K921.txt

10-Strike Network Inventory Explorer Pro 9.05 - Buffer Overflow (SEH)
| windows/local/493[01;31m[K22[m[K.py

12Planet Chat Server 2.5 - Error Message Installation Full Path Disclosure |
multiple/remote/[01;31m[K22[m[K497.txt

2Moons 1.4 - Multiple Remote File Inclusions
| php/webapps/36[01;31m[K22[m[K3.txt

2WIRE Gateway - Authentication Bypass / Password Reset (1)
| hardware/remote/94[01;31m[K22[m[K.txt

2WIRE Modems/Routers - 'CRLF' Denial of Service
| hardware/dos/[01;31m[K22[m[K46.cpp

3Com DSL Router 812 1.1.7/1.1.9/2.0 - Administrative Interface Long Request Denial of Service |
hardware/dos/[01;31m[K22[m[K947.c

3Com OfficeConnect Wireless Cable/DSL Router - Authentication Bypass
| hardware/remote/80[01;31m[K22[m[K.txt

3Com SuperStack 3 Firewall - Content Filter Bypassing
| multiple/remote/[01;31m[K22[m[K327.txt

3Com SuperStack 3 NBX 4.0/4.1 - FTPD Denial of Service
| hardware/dos/[01;31m[K22[m[K060.txt

3Com SuperStack II RAS 1500 - IP Header Denial of Service
| hardware/dos/[01;31m[K22[m[K415.c

3Com SuperStack II RAS 1500 - Unauthorized Access
| hardware/remote/[01;31m[K22[m[K416.txt

3D-FTP Client 4.0 - Buffer Overflow
| windows/dos/[01;31m[K22[m[K551.pl

3proxy 0.5.3g (Windows x86) - 'proxy.c logurl()' Remote Buffer Overflow
| windows_x86/remote/38[01;31m[K22[m[K.c

3ware Disk Managment 1.10 - HTTP Request Denial of Service
| multiple/dos/[01;31m[K22[m[K207.txt

4homepages 4Images 1.7.x - 'categories.php' SQL Injection
| php/webapps/350[01;31m[K22[m[K.txt

60 cycleCMS 2.5.2 - Cross-Site Request Forgery (Change Username and
Password) |
php/webapps/1[01;31m[K22[m[K66.txt

60cycleCMS 2.5.2 - 'DOCUMENT_ROOT' Multiple Local File Inclusions
| php/webapps/1[01;31m[K22[m[K49.txt

68KB Knowledge Base 1.0.0rc3 - Cross-Site Request Forgery (Edit Main
Settings) |
php/webapps/120[01;31m[K22[m[K.txt

6KBBS 8.0 build 20101201 - Cross-Site Scripting / Information
Disclosure |
php/webapps/36[01;31m[K22[m[K4.txt

ABB Cylon Aspect 3.07.02 (userManagement.php) - Weak Password Policy
| multiple/hardware/5[01;31m[K22[m[K21.txt

ABB Cylon Aspect 3.08.02 (bbmdUpdate.php) - Remote Code Execution
| multiple/hardware/5[01;31m[K22[m[K17.txt

ABB Cylon Aspect 3.08.02 (deployStart.php) - Unauthenticated Command
Execution |
php/hardware/5[01;31m[K22[m[K51.txt

ABB Cylon Aspect 3.08.02 (escDevicesUpdate.php) - Denial of Service
(DOS) |
php/hardware/5[01;31m[K22[m[K18.txt

ABB Cylon Aspect 3.08.02 (ethernetUpdate.php) - Authenticated Path
Traversal |
php/hardware/5[01;31m[K22[m[K52.txt

ABB Cylon Aspect 3.08.02 (licenseServerUpdate.php) - Stored Cross-Site Scripting |
multiple/hardware/5[01;31m[K22[m[K14.txt

ABB Cylon Aspect 3.08.02 (licenseUpload.php) - Stored Cross-Site Scripting |
multiple/hardware/5[01;31m[K22[m[K15.txt

ABB Cylon Aspect 3.08.02 (uploadDb.php) - Remote Code Execution
| multiple/hardware/5[01;31m[K22[m[K16.txt

ABB Cylon Aspect 3.08.02 (webServerUpdate.php) - Input Validation Config Poisoning |
php/hardware/5[01;31m[K22[m[K19.txt

ABB Cylon Aspect 3.08.02 - Cookie User Password Disclosure
| multiple/hardware/5[01;31m[K22[m[K24.txt

ABB Cylon Aspect 3.08.02 - Cross-Site Request Forgery (CSRF)
| multiple/hardware/5[01;31m[K22[m[K31.html

ABB Cylon Aspect 3.08.03 (CookieDB) - SQL Injection
| multiple/hardware/5[01;31m[K22[m[K20.txt

ABB Cylon Aspect 3.08.03 (MapServicesHandler) - Authenticated Reflected XSS |
multiple/webapps/5[01;31m[K22[m[K[01;31m[K22[m[K.txt

ABB Cylon Aspect 3.08.03 (webServerDeviceLabelUpdate.php) - File Write DoS |
php/hardware/5[01;31m[K22[m[K34.txt

ABB Cylon Aspect 3.08.03 - Hard-coded Secrets
| multiple/webapps/5[01;31m[K22[m[K23.txt

ABB Cylon Aspect 4.00.00 (factorySaved.php) - Unauthenticated XSS
| php/hardware/5[01;31m[K22[m[K33.txt

ABB Cylon Aspect 4.00.00 (factorySetSerialNum.php) - Remote Code Execution |
php/hardware/5[01;31m[K22[m[K32.txt

Ability Mail Server 2013 -Persistent Cross-Site Scripting / Cross-Site Request Forgery (Password Reset) |
windows/webapps/31[01;31m[K22[m[K1.txt

abrt (Centos 7.1 / Fedora [01;31m[K22[m[K) - Local Privilege Escalation
| multiple/local/38835.py

Abuse-SDL 0.7 - Command Line Argument Buffer Overflow
| bsd/local/[01;31m[K22[m[K811.c

```
Abyss Web Server 1.1.2 - Incomplete HTTP Request Denial of Service
| windows/dos/[01;31m[K22[m[K460.txt

ac4p Mobile - 'polls.php' Multiple Cross-Site Scripting Vulnerabilities
(2)                                | php/webapps/29[01;31m[K22[m[K6.txt

ac4p Mobile - 'up.php?Taaa' Cross-Site Scripting
| php/webapps/29[01;31m[K22[m[K5.txt

Accellion File Transfer - 'Appliance web_client_user_guide.html?lang'
Traversal Arbitrary File Access      |
linux/remote/336[01;31m[K22[m[K.txt

Accellion File Transfer - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K22[m[K90.txt

acFTP 1.4 - Invalid Password Weak Authentication
| windows/remote/[01;31m[K22[m[K032.txt

Achievo 1.4.5 - Multiple Vulnerabilities (1)
| php/webapps/[01;31m[K22[m[K431.txt

ACME Labs thttpd 2.20 - Cross-Site Scripting
| linux/remote/214[01;31m[K22[m[K.txt

Acme thttpd HTTP Server - Directory Traversal
| linux/remote/385[01;31m[K22[m[K.txt

Acoustica 3.32 CD/DVD Label Maker - '.m3u' (PoC)
| windows/dos/124[01;31m[K22[m[K.pl

Acoustica Mixcraft 4.2 Build 98 - 'mx4' Local Buffer Overflow
| windows/local/63[01;31m[K22[m[K.pl

Acpid 1:2.0.10-1ubuntu2 (Ubuntu 11.04/11.10) - Boundary Crossing
Privilege Escalation                        |
linux/local/18[01;31m[K22[m[K8.sh

acronis pxe server 2.0.0.1076 - Directory Traversal / Null Pointer
| windows/remote/5[01;31m[K22[m[K8.txt

ActFax Server (LPD/LPR) 4.25 Build 0[01;31m[K22[m[K1 (2010-02-11) -
Remote Buffer Overflow                                  |
windows/remote/16176.pl

ActFax Server 4.31 Build 0[01;31m[K22[m[K5 - Local Privilege Escalation
| windows/local/20915.py

ActFax Server FTP 4.25 Build 0[01;31m[K22[m[K1 (2010-02-11) -
(Authenticated) Remote Buffer Overflow                    |
windows/remote/16177.py
```

```
ACTi ASOC [01;31m[K22[m[K00 Web Configurator 2.6 - Remote Command
Execution                                                 |
hardware/remote/16993.pl

Active eCommerce CMS 6.5.0 - Stored Cross-Site Scripting (XSS)
| multiple/webapps/51[01;31m[K22[m[K1.txt

ActiveMQ < 5.14.0 - Web Shell Upload (Metasploit)
| java/remote/4[01;31m[K22[m[K83.rb

Activity Monitor 2002 2.6 - Remote Denial of Service
| windows/dos/[01;31m[K22[m[K690.c

Acuity CMS 2.6.2 - '/admin/file_manager/browse.asp?path' Traversal
Arbitrary File Access                    |
asp/webapps/37[01;31m[K22[m[K3.txt

Acuity CMS 2.6.2 - '/admin/file_manager/file_upload_submit.asp'
Multiple Arbitrary File Upload / Code Exec |
asp/webapps/37[01;31m[K22[m[K2.txt

Ad Board Script 1.01 - Local File Inclusion
| php/webapps/117[01;31m[K22[m[K.txt

AD Manager Plus 71[01;31m[K22[m[K - Remote Code Execution (RCE)
| java/remote/51183.txt

Adapt Authoring Tool 0.11.3 - Remote Command Execution (RCE)
| multiple/webapps/5[01;31m[K22[m[K08.py

AdMan 1.0.20051[01;31m[K22[m[K1 - 'ViewStatement.php' SQL Injection
| php/webapps/27462.txt

Admidio 3.3.5 - Cross-Site Request Forgery (Change Permissions)
| php/webapps/453[01;31m[K22[m[K.txt

Adobe - U3D CLODProgressiveMeshDeclaration Array Overrun (Metasploit)
(2)                                  |
windows/local/166[01;31m[K22[m[K.rb

Adobe Acrobat 7.0 / Adobe Reader 7.0 - File Existence / File Disclosure
| windows/remote/258[01;31m[K22[m[K.xml

Adobe Acrobat 9.1.2 NOS - Local Privilege Escalation
| windows/local/9[01;31m[K22[m[K3.txt

Adobe Acrobat Reader (UNIX) 5.0 6 / Xpdf 0.9x Hyperlinks - Arbitrary
Command Execution                        |
linux/remote/[01;31m[K22[m[K771.txt

Adobe Flash (Multiple Scripts) - Use-After-Free When Rendering Displays
(1)                                  | windows/dos/39[01;31m[K22[m[K0.txt
```

Adobe Flash - ATF Parser Heap Corruption
| multiple/dos/4[01;31m[K22[m[K49.txt

Adobe Flash - AVC Edge Processing Out-of-Bounds Read
| multiple/dos/4[01;31m[K22[m[K47.txt

Adobe Flash - Image Decoding Out-of-Bounds Read
| multiple/dos/4[01;31m[K22[m[K48.txt

Adobe Flash - Use-After-Free in Applying Bitmap Filter
| multiple/dos/414[01;31m[K22[m[K.txt

Adobe Flash - Use-After-Free When Setting Stage
| windows_x86-64/dos/39[01;31m[K22[m[K1.txt

Adobe Flash GradientFill - Use-After-Frees
| windows/dos/390[01;31m[K22[m[K.txt

Adobe Flash Player 10.0.[01;31m[K22[m[K / AIR - 'intf_count' Integer
Overflow |
linux/dos/33134.txt

Adobe Flash Player 10.0.[01;31m[K22[m[K / AIR - URI Parsing Heap Buffer
Overflow (PoC) |
multiple/dos/33133.txt

Adobe Flash Player [01;31m[K22[m[K.0.0.192 - DefineBitsJPEG2 Memory
Corruption |
multiple/dos/40102.txt

Adobe Flash Player [01;31m[K22[m[K.0.0.192 - DefineSprite Memory
Corruption |
multiple/dos/40103.txt

Adobe Flash Player [01;31m[K22[m[K.0.0.192 - SceneAndFrameData Memory
Corruption |
multiple/dos/40104.txt

Adobe Flash Player [01;31m[K22[m[K.0.0.192 - TAG Memory Corruption
| multiple/dos/40105.txt

Adobe Reader 10.1.4 - Crash (PoC)
| windows/dos/[01;31m[K22[m[K155.pl

Adobe Reader 10.1.4 - JP2KLib&CoolType Crash (PoC)
| windows/dos/[01;31m[K22[m[K878.txt

Adobe Reader 11.0.0 - Stack Overflow Crash (PoC)
| windows/dos/[01;31m[K22[m[K464.txt

Adobe Unix Acrobat Reader 4.0/5.0 - WWWLaunchNetscape Buffer Overflow
| linux/dos/[01;31m[K22[m[K846.pl

```
Advaced-Clan-Script 3.4 - 'mcf.php' Remote File Inclusion
| php/webapps/24[01;31m[K22[m[K.txt

Advanced Poll 2.0 - Remote Information Disclosure
| php/webapps/[01;31m[K22[m[K412.txt

Advanced Real Estate Script 4.0.6 - SQL Injection
| php/webapps/415[01;31m[K22[m[K.txt

Aero CMS v0.0.1 - SQLi
| php/webapps/510[01;31m[K22[m[K.txt

AFCommerce - 'controlheader.php' Remote File Inclusion
| php/webapps/389[01;31m[K22[m[K.txt

Aiglon Web Server 2.0 - Installation Path Information Disclosure
| multiple/remote/[01;31m[K22[m[K755.txt

AIOCP 1.3.x - 'load_page' Remote File Inclusion
| php/webapps/289[01;31m[K22[m[K.txt

Aircrack-NG Tools svn r1675 - Remote Heap Buffer Overflow (PoC)
| multiple/dos/1[01;31m[K22[m[K17.py

AIX 3.x/4.x / Windows 95/98/2000/NT 4.0 / SunOS 5 - 'gethostbyname()'
Remote Buffer Overflow               |
multiple/remote/[01;31m[K22[m[K251.sh

Aladdin Knowledge System Ltd - 'ChooseFilePath' Remote Buffer Overflow
(Metasploit)                         |
windows/remote/[01;31m[K22[m[K375.rb

Aladdin Knowledge System Ltd - 'PrivAgent.ocx' ChooseFilePath Buffer
Overflow                              |
windows/remote/[01;31m[K22[m[K301.html

Aladdin Knowledge System Ltd. PrivAgent ActiveX Control 2.0 - Multiple
Vulnerabilities                      |
windows/dos/[01;31m[K22[m[K258.txt

AlberT-EasySite 1.0a5 - 'PSA_PATH' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K60.pl

Alcassoft's SOPHIA CMS - SQL Injection
| cfm/webapps/16[01;31m[K22[m[K5.txt

Alegro 1.2.1 - SQL Injection
| php/webapps/1[01;31m[K22[m[K78.txt

Alguest 1.1c-patched - 'elimina' SQL Injection
| php/webapps/35[01;31m[K22[m[K7.txt
```

```
alitalk 1.9.1.1 - Multiple Vulnerabilities
| php/webapps/49[01;31m[K22[m[K.txt

All4WWW-HomePageCreator 1.0 - 'index.php' Remote File Inclusion
| php/webapps/254[01;31m[K22[m[K.txt

Allaire ColdFusion Server 4.0.1 - 'CFCRYPT.EXE' Decrypt Pages
| windows/local/19[01;31m[K22[m[K0.c

Allinta CMS [01;31m[K22[m[K.07.2010 - Multiple SQL Injections / Cross-
Site Scripting Vulnerabilities                    |
asp/webapps/34429.txt

Almnzm 2.1 - SQL Injection
| php/webapps/1[01;31m[K22[m[K20.txt

Aloaha Credential Provider Monitor 5.0.[01;31m[K22[m[K6 - Local
Privilege Escalation                                    |
windows/local/24258.txt

Alt-N MDaemon 3.1.1 - Denial of Service
| windows/dos/20[01;31m[K22[m[K5.pl

Alt-N MDaemon POP3 Server < 9.06 - 'USER' Remote Heap Overflow
| windows/remote/[01;31m[K22[m[K58.py

Alt-N WebAdmin 2.0.x - 'USER' Remote Buffer Overflow (1)
| windows/remote/[01;31m[K22[m[K833.c

Alt-N WebAdmin 2.0.x - 'USER' Remote Buffer Overflow (2)
| windows/remote/[01;31m[K22[m[K834.c

Alt-N WebAdmin 2.0.x - Remote File Disclosure
| cgi/remote/[01;31m[K22[m[K542.txt

Alt-N WebAdmin 2.0.x - Remote File Viewing
| cgi/remote/[01;31m[K22[m[K541.txt

Amavis 0.1.6 - Header Parsing Mail Relaying
| unix/remote/[01;31m[K22[m[K475.txt

AMX Mod 0.9.2 - Remote 'amx_say' Format String
| linux/remote/[01;31m[K22[m[K291.c

AN HTTPD 1.41 e - Cross-Site Scripting
| multiple/remote/[01;31m[K22[m[K130.txt

AN HTTPD 1.x - Count.pl Directory Traversal
| windows/remote/[01;31m[K22[m[K515.txt

Angular-Base64-Upload Library 0.1.21 - Unauthenticated Remote Code
Execution (RCE)                          |
multiple/webapps/5[01;31m[K22[m[K53.py
```

```
Annuaire 1Two 2.2 - SQL Injection
| php/webapps/[01;31m[K22[m[K89.pl

AnotherPHPBook (APB) 1.3.0 - Authentication Bypass
| php/webapps/9[01;31m[K22[m[K5.txt

Antelope Software W4-Server 2.6 a/Win32 - 'Cgitest.exe' Remote Buffer
Overflow                                |
windows/remote/196[01;31m[K22[m[K.c

antMan < 0.9.1a - Authentication Bypass
| multiple/webapps/44[01;31m[K22[m[K0.txt

AnyDesk 9.0.1 - Unquoted Service Path
| windows/local/5[01;31m[K22[m[K58.txt

Apache - Denial of Service
| linux/dos/18[01;31m[K22[m[K1.c

Apache 1.3.x + Tomcat 4.0.x/4.1.x mod_jk - Chunked Encoding Denial of
Service                                 | unix/dos/[01;31m[K22[m[K068.pl

Apache < 1.3.37/2.0.59/2.2.3 mod_rewrite - Remote Overflow
| multiple/remote/[01;31m[K22[m[K37.sh

Apache ActiveMQ 6.1.6 - Denial of Service (DOS)
| multiple/remote/5[01;31m[K22[m[K88.py

Apache Commons Text  1.10.0 - Remote Code Execution
| multiple/webapps/5[01;31m[K22[m[K61.py

Apache Geronimo 2.1.x - Cross-Site Request Forgery (Multiple Admin
Function)                                 |
multiple/remote/329[01;31m[K22[m[K.html

Apache Mod_Access_Referer 1.0.2 - Null Pointer Dereference Denial of
Service                                  |
multiple/dos/[01;31m[K22[m[K505.txt

Apache OFBiz - Admin Creator
| multiple/remote/1[01;31m[K22[m[K64.txt

Apache OFBiz - Remote Execution (via SQL Execution)
| multiple/remote/1[01;31m[K22[m[K63.txt

Apache Subversion - Remote Denial of Service
| linux/dos/384[01;31m[K22[m[K.txt

Apache Tomcat 3.x - Null Byte Directory / File Disclosure
| linux/remote/[01;31m[K22[m[K205.txt

Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)
| multiple/remote/6[01;31m[K22[m[K9.txt
```

Apache Web Server 2.0.x - MS-DOS Device Name Denial of Service
| linux/dos/[01;31m[K22[m[K191.pl

APBoard 2.0 2 - Unauthorized Thread Reading
| php/webapps/[01;31m[K22[m[K073.txt

Apple iTouch/iPhone 1.1.1 - '.tif' Remote Privilege Escalation
'Jailbreak' |
ios/remote/45[01;31m[K22[m[K.html

Apple iTunes 10.6.1.7 - Extended m3u Stack Buffer Overflow (Metasploit)
| windows/remote/193[01;31m[K22[m[K.rb

Apple Mac OSX 10.2.2 - Directory Kernel Panic (Denial of Service)
| osx/dos/[01;31m[K22[m[K074.txt

Apple Mac OSX 10.x - DirectoryService Denial of Service
| osx/dos/[01;31m[K22[m[K483.c

Apple Mac OSX Kernel - Null Pointer Dereference in AppleMuxControl.kext
| osx/dos/399[01;31m[K22[m[K.c

Apple Mac OSX xnu 1[01;31m[K22[m[K8.0 - 'mach-o' Local Kernel Denial of
Service (PoC) | osx/dos/4689.c

Apple Mac OSX xnu 1[01;31m[K22[m[K8.0 - 'super_blob' Local kernel
Denial of Service (PoC) | osx/dos/4723.c

Apple Mac OSX xnu 1[01;31m[K22[m[K8.3.13 - 'macfsstat' Local Kernel
Memory Leak/Denial of Service | osx/dos/8263.c

Apple Mac OSX xnu 1[01;31m[K22[m[K8.3.13 - 'Profil' Kernel Memory
Leak/Denial of Service (PoC) | osx/dos/8264.c

Apple Mac OSX xnu 1[01;31m[K22[m[K8.3.13 - 'zip-notify' Remote Kernel
Overflow (PoC) | osx/dos/8262.c

Apple Mac OSX xnu 1[01;31m[K22[m[K8.3.13 - IPv6-ipcomp Remote kernel
Denial of Service (PoC) |
multiple/dos/5191.c

Apple Mac OSX xnu 1[01;31m[K22[m[K8.9.59 - Kernel Privilege Escalation
| osx/local/8896.c

Apple Mac OSX xnu 1[01;31m[K22[m[K8.x - 'hfs-fcntl' Kernel Privilege
Escalation | osx/local/8266.sh

Apple Mac OSX xnu 1[01;31m[K22[m[K8.x - 'vfssysctl' Local Kernel Denial
of Service (PoC) | osx/dos/8265.c

Apple Mac OSX xnu 1[01;31m[K22[m[K8.x - Local Kernel Memory Disclosure
| osx/local/8108.c

Apple QuickTime 7.7.2 - MIME Type Buffer Overflow (Metasploit)
| windows/remote/[01;31m[K22[m[K973.rb

Apple QuickTime 7.7.2 - Targa image Buffer Overflow
| windows/dos/[01;31m[K22[m[K855.txt

Apple QuickTime 7.7.2 - TeXML Style Element font-table Field Stack
Buffer Overflow (Metasploit) |
windows/remote/[01;31m[K22[m[K905.rb

Apple QuickTime Player 7.7.2 - Crash (PoC)
| windows/dos/[01;31m[K22[m[K214.pl

Apple QuickTime/Darwin Streaming MP3Broadcaster - ID3 Tag Handling
| osx/remote/[01;31m[K22[m[K630.txt

Apple QuickTime/Darwin Streaming Server 4.1.3 QTSSReflector Module -
Integer Overflow | osx/dos/[01;31m[K22[m[K629.txt

Apple QuickTime/Darwin Streaming Server 4.1.x - 'parse_xml.cgi' File
Disclosure |
cgi/remote/[01;31m[K22[m[K312.txt

Apple Safari 4.0.5 (531.[01;31m[K22[m[K.7) - Denial of Service
| windows/dos/12408.pl

Apple watchOS 2 - Crash (PoC)
| hardware/dos/39[01;31m[K22[m[K5.txt

Apple WebCore - XMLHTTPRequest Cross-Site Scripting
| osx/remote/30[01;31m[K22[m[K8.txt

appRain CMF - Arbitrary '.PHP' File Upload (Metasploit)
| php/webapps/189[01;31m[K22[m[K.rb

ArcademSX 2.904 - 'cat' Cross-Site Scripting
| php/webapps/34[01;31m[K22[m[K9.txt

Archive Searcher - '.zip' Local Stack Overflow
| windows/local/1[01;31m[K22[m[K61.rb

ArGoSoft 1.8.x - Authentication Bypass
| windows/remote/[01;31m[K22[m[K604.txt

ArGoSoft Mail Server 1.8.3.5 - GET Multiple Denial of Service
Vulnerabilities |
windows/dos/[01;31m[K22[m[K757.c

Armida Databased Web Server 1.0 - GET Remote Denial of Service
| windows/dos/[01;31m[K22[m[K825.c

Article Directory - 'index.php' Remote File Inclusion
| php/webapps/4[01;31m[K22[m[K1.txt

```
asg-sentry 7.0.0 - Multiple Vulnerabilities
| multiple/dos/5[01;31m[K22[m[K9.txt

ASP-DEV Discussion Forum 2.0 - Admin Directory Weak Default Permissions
| asp/webapps/[01;31m[K22[m[K895.txt

ASPBB 0.4 - 'forum.asp?FORUM_ID' SQL Injection
| asp/webapps/268[01;31m[K22[m[K.txt

ASPCode CMS 1.5.8 - 'default.asp' Multiple Cross-Site Scripting
Vulnerabilities                              |
asp/webapps/337[01;31m[K22[m[K.txt

Asterisk < 1.2.[01;31m[K22[m[K/1.4.8 - IAX2 Channel Driver Remote Crash
| multiple/dos/4249.rb

Asterisk < 1.2.[01;31m[K22[m[K/1.4.8/2.2.1 - 'chan_skinny' Remote
Denial of Service                                        |
multiple/dos/4196.c

Asterisk PBX 0.7.x - Multiple Logging Format String Vulnerabilities
| linux/remote/24[01;31m[K22[m[K1.pl

ASUS AAHM 1.00.[01;31m[K22[m[K - 'asHmComSvc' Unquoted Service Path
| windows/local/48206.txt

Asus AAM6330BI/AAM6000EV ADSL Router - Information Disclosure
| hardware/remote/[01;31m[K22[m[K898.txt

ASUS ASMB8 iKVM 1.14.51 - Remote Code Execution (RCE)
| hardware/local/5[01;31m[K22[m[K44.txt

Asus Precision TouchPad 11.0.0.25 - Denial of Service
| windows/dos/473[01;31m[K22[m[K.py

AT 3.1.8 - Formatted Time Heap Overflow
| linux/local/21[01;31m[K22[m[K9.txt

Atar2b CMS 4.0.1 - 'pageH.php?id' SQL Injection
| php/webapps/365[01;31m[K22[m[K.txt

ATFTP 0.7 - Timeout Command Line Argument Local Buffer Overflow
| linux/local/[01;31m[K22[m[K768.pl

Atlassian JIRA FishEye 2.5.7 / Crucible 2.5.7 Plugins - XML Parsing
Security                                  |
jsp/webapps/37[01;31m[K22[m[K1.txt

atomicboard 0.6.2 - Directory Traversal
| php/webapps/[01;31m[K22[m[K941.txt

ATutor 1.2 - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K160.txt
```

Audacity 1.2.6 - '.gro' Local Buffer Overflow
| windows/local/103[01;31m[K22[m[K.py

AudioCoder 0.8.[01;31m[K22[m[K - '.lst' Direct RETN Buffer Overflow
| windows/local/26448.py

AudioCoder 0.8.[01;31m[K22[m[K - '.m3u' Direct RETN Buffer Overflow
| windows/local/26411.py

AudioCoder 0.8.[01;31m[K22[m[K - '.m3u' Local Buffer Overflow (SEH)
| windows/local/29309.pl

Australian Education App - Remote Code Execution
| android/remote/4[01;31m[K22[m[K89.txt

AutomatedShops WebC 2.0/5.0 - Symbolic Link Following Configuration File |
linux/local/[01;31m[K22[m[K456.txt

AutomatedShops WebC 2.0/5.0 Script - Name Remote Buffer Overrun
| linux/remote/[01;31m[K22[m[K454.c

AvailScript Article Script - 'view.php' SQL Injection
| php/webapps/65[01;31m[K22[m[K.txt

Avast aswSnx.sys Kernel Driver 11.1.[01;31m[K22[m[K53 - Memory Corruption Privilege Escalation |
windows/dos/42182.cpp

AVAST SecureLine 5.5.5[01;31m[K22[m[K.0 - 'SecureLine' Unquoted Service Path |
windows/local/48249.txt

Avaya Cajun P130/P133/P330/P333 Network Switch - Connection Stalling Denial of Service |
hardware/dos/[01;31m[K22[m[K797.txt

AVE DOMINAplus 1.10.x - Authentication Bypass
| hardware/webapps/478[01;31m[K22[m[K.txt

AVerCaster Pro RS3400 Web Server - Directory Traversal
| hardware/webapps/[01;31m[K22[m[K549.txt

Aviosoft Digital TV Player Professional 1.x - '.PLF' Direct Retn
| windows/local/[01;31m[K22[m[K932.py

Avira AntiVir Personal - Multiple Code Execution Vulnerabilities (1)
| windows/remote/35[01;31m[K22[m[K5.c

Avira AntiVir Personal - Multiple Code Execution Vulnerabilities (2)
| windows/remote/35[01;31m[K22[m[K6.py

```
Avtech Software - ActiveX 'avc781viewer.dll' Multiple Vulnerabilities
| windows/dos/1[01;31m[K22[m[K94.txt

AWStats 6.8 - 'AWStats.pl' Cross-Site Scripting
| cgi/webapps/3[01;31m[K22[m[K58.txt

Axessh 4.2 - 'Log file name' Local Stack-based Buffer Overflow
| windows/local/469[01;31m[K22[m[K.py

Axigen < 10.3.3.47_ 10.2.3.12 - Reflected XSS
| multiple/webapps/517[01;31m[K22[m[K.txt

Axigen Webmail 1.0.1 - Directory Traversal
| windows/remote/346[01;31m[K22[m[K.txt

Axis Communications HTTP Server 2.x - Messages Information Disclosure
| multiple/remote/[01;31m[K22[m[K296.txt

Axis Communications Video Server 2.x - 'Command.cgi' File Creation
| cgi/remote/[01;31m[K22[m[K311.txt

Axis Network Camera 2.x - HTTP Authentication Bypass
| hardware/remote/[01;31m[K22[m[K626.txt

Axis Print Server 6.15/6.20 - Web Interface Denial of Service
| multiple/dos/[01;31m[K22[m[K859.txt

Ay System CMS 2.6 - 'main.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K63.txt

Azure Apache Ambari 230[01;31m[K22[m[K50400 - Spoofing
| multiple/remote/51546.py

b1gbb 2.24.0 - SQL Injection / Cross-Site Scripting
| php/webapps/41[01;31m[K22[m[K.txt

BabyGekko 1.2.2e - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K741.txt

Backup and Staging by WP Time Capsule 1.[01;31m[K22[m[K.21 -
Unauthenticated Arbitrary File Upload                        |
php/webapps/52131.py

Bananadance Wiki b2.2 - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K654.txt

Bandmin 1.4 - Cross-Site Scripting
| cgi/webapps/[01;31m[K22[m[K669.txt

BandSite CMS 1.1 - 'login_header.php' Cross-Site Scripting
| php/webapps/286[01;31m[K22[m[K.txt
```

Barcodes generator 1.0 - 'name' Stored Cross Site Scripting
| php/webapps/49[01;31m[K22[m[K7.txt

Basic Analysis and Security Engine (BASE) 1.4.5 -
'/includes/base_state_common.inc.php?GLOBALS[user_sessio |
php/webapps/367[01;31m[K22[m[K.txt

Basit 1.0 Search Module - Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K385.txt

Basit 1.0 Submit Module - Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K383.txt

BaSoMail 1.24 - POP3 Server Denial of Service
| windows/dos/[01;31m[K22[m[K667.txt

BaSoMail 1.24 - SMTP Server Command Buffer Overflow
| windows/dos/[01;31m[K22[m[K668.txt

Batalla Naval 1.0 4 - Remote Buffer Overflow (1)
| linux/remote/[01;31m[K22[m[K658.pl

Batalla Naval 1.0 4 - Remote Buffer Overflow (2)
| linux/remote/[01;31m[K22[m[K659.c

Battleaxe Software BTTLXE Forum - 'login.asp' SQL Injection
| asp/webapps/[01;31m[K22[m[K529.txt

Battlefield (BFCC < 1.[01;31m[K22[m[K_A /BFVCC < 2.14_B / BF2CC) -
Authentication Bypass / Password Stealer / Denial of |
windows/remote/1183.c

BEA AquaLogic Interaction 6.0/6.1 Plumtree Portal - Multiple
Information Disclosure Vulnerabilities |
php/webapps/308[01;31m[K22[m[K.txt

BEA WebLogic 7.0 - Hostname/NetBIOS Name Remote Information Disclosure
| windows/remote/[01;31m[K22[m[K448.txt

Beanwebb Guestbook 1.0 - Unauthorized Administrative Access
| php/webapps/[01;31m[K22[m[K443.txt

Belkin F9K11[01;31m[K22[m[Kv1 1.00.30 - Buffer Overflow (via Cross-Site
Request Forgery) |
hardware/webapps/40332.py

Best Support System 3.0.4 - 'ticket_body' Persistent XSS
(Authenticated) |
php/webapps/491[01;31m[K22[m[K.txt

BestSafe Browser - Man In The Middle Remote Code Execution
| android/remote/4[01;31m[K22[m[K88.txt

bfcommand & control server 1.[01;31m[K22[m[K/2.0/2.14 manager - Multiple Vulnerabilities | multiple/remote/26210.txt

BFTPd 1.0.12 - Remote Overflow | linux/remote/[01;31m[K22[m[K5.c

bgERP v[01;31m[K22[m[K.31 (Orlovets) - Cookie Session vulnerability & Cross-Site Scripting (XSS) | php/webapps/51245.txt

BigAnt Server 2.52 SP5 - Remote Stack Overflow ROP-Based (SEH) (ASLR + DEP Bypass) | windows/remote/[01;31m[K22[m[K466.py

Bild Flirt System 1.0 - SQL Injection | php/webapps/1[01;31m[K22[m[K21.rb

BIND 9.4.1 < 9.4.2 - Remote DNS Cache Poisoning (Metasploit) | multiple/remote/61[01;31m[K22[m[K.rb

BitchX 1.0 - 'RPL_NAMREPLY' Denial of Service | linux/dos/[01;31m[K22[m[K259.c

BitchX 1.0 - Remote 'Send_CTCP()' Memory Corruption | linux/remote/[01;31m[K22[m[K353.c

BitMover BitKeeper 3.0 - Daemon Mode Remote Command Execution | multiple/remote/[01;31m[K22[m[K145.txt

Bitweaver 2.8.1 - Multiple Vulnerabilities | php/webapps/[01;31m[K22[m[K216.txt

BizDesign ImageFolio 2.x/3.0.1 - 'imageFolio.cgi?direct' Cross-Site Scripting | cgi/webapps/[01;31m[K22[m[K050.txt

BizDesign ImageFolio 2.x/3.0.1 - 'nph-build.cgi' Cross-Site Scripting | cgi/webapps/[01;31m[K22[m[K051.txt

BlazeBoard 1.0 - Information Disclosure | php/webapps/[01;31m[K22[m[K901.txt

BlazeVideo HDTV Player 6.6 Professional - Direct RETN | windows/local/[01;31m[K22[m[K931.py

BLNews 2.1.3 - Remote File Inclusion | php/webapps/[01;31m[K22[m[K641.txt

BlogEngine 3.3 - 'syndication.axd' XML External Entity Injection | xml/webapps/484[01;31m[K22[m[K.txt

Blood Bank & Donor Management System 2.4 - CSRF Improper Input Validation |
multiple/webapps/5[01;31m[K22[m[K56.txt

blueimp's jQuery 9.[01;31m[K22[m[K.0 - (Arbitrary) File Upload (Metasploit) |
php/remote/45790.rb

Blueimp's jQuery File Upload 9.[01;31m[K22[m[K.0 - Arbitrary File Upload Exploit |
php/webapps/46182.py

Bluemoon inc. PopnupBlog 3.30 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/3[01;31m[K22[m[K96.txt

BlueSocket BSC 2100 5.0/5.1 - Admin.pl Cross-Site Scripting
| cgi/webapps/29[01;31m[K22[m[K1.txt

BM Classifieds 20080409 - Multiple SQL Injections
| php/webapps/5[01;31m[K22[m[K3.txt

BMC Software Patrol 3.2.5 - Patrol SNMP Agent File Creation/Permission
| linux/local/194[01;31m[K22[m[K.txt

BOA Web Server 0.94.14rc21 - Arbitrary File Access
| linux/webapps/4[01;31m[K22[m[K90.txt

Booby 1.0.1 - Multiple Remote File Inclusions
| php/webapps/57[01;31m[K22[m[K.txt

Book Library 1.4.162 - '.bkd' Local Denial of Service
| windows/dos/1[01;31m[K22[m[K29.py

Boozt Standard 0.9.8 - 'index.cgi' Buffer Overrun
| cgi/remote/[01;31m[K22[m[K054.c

BoxBilling<=4.[01;31m[K22[m[K.1.5 - Remote Code Execution (RCE)
| php/webapps/51108.txt

Broadcom BCM4325 / BCM4329 Devices - Denial of Service
| hardware/dos/[01;31m[K22[m[K739.py

BRS Webweaver 1.0 - Error Page Cross-Site Scripting
| windows/remote/[01;31m[K22[m[K838.txt

BRS Webweaver 1.0 1 - MKDir Directory Traversal
| linux/remote/[01;31m[K22[m[K143.txt

BRS Webweaver 1.0 4 - POST / HEAD Denial of Service
| multiple/dos/[01;31m[K22[m[K650.py

```
Bs Auto_Classifieds Script - 'articlesdetails.php' SQL Injection
| php/webapps/14[01;31m[K22[m[K9.txt

Bs Events_Locator Script - SQL Injection
| php/webapps/14[01;31m[K22[m[K7.txt

Bs General_Classifieds Script - SQL Injection
| php/webapps/14[01;31m[K22[m[K8.txt

Bs Home_Classifieds Script - SQL Injection
| php/webapps/14[01;31m[K22[m[K6.txt

Bs Realtor_Web Script - SQL Injection
| php/webapps/14[01;31m[K22[m[K5.txt

Bs Recipes_Website Script - SQL Injection / Authentication Bypass
| php/webapps/14[01;31m[K22[m[K4.txt

Bs Scripts_Directory - SQL Injection / Authentication Bypass
| php/webapps/14[01;31m[K22[m[K3.txt

BSD 'lpr' 2000.05.07/0.48/0.72 / lpr-ppd 0.72 - Local Buffer Overflow
(1)                                  | unix/local/[01;31m[K22[m[K331.c

BSD 'lpr' 2000.05.07/0.48/0.72 / lpr-ppd 0.72 - Local Buffer Overflow
(2)                                  | unix/local/[01;31m[K22[m[K332.c

BugFree 2.1.3 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/36[01;31m[K22[m[K8.txt

Bugzilla 3.1.4 - '--attach_path' Directory Traversal
| linux/remote/3[01;31m[K22[m[K28.xml

BulletProof FTP Server 2019.0.0.50 - 'SMTP Server' Denial of Service
(PoC)                                 |
windows/dos/464[01;31m[K22[m[K.py

BuyClassifiedScript - PHP Code Injection
| php/webapps/[01;31m[K22[m[K929.txt

ByteCatcher FTP Client 1.0.4 - 'Server Banner' Buffer Overflow
| windows/dos/[01;31m[K22[m[K[01;31m[K22[m[K0.pl

BZFlag 1.7 g0 - Reconnect Denial of Service
| linux/dos/[01;31m[K22[m[K624.c

C-Cart 1.0 - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K995.txt

CA Total Defense Suite - reGenerateReports Stored procedure SQL
Injection (Metasploit)                    |
cgi/webapps/179[01;31m[K22[m[K.rb
```

```
Cacti 1.2.26 -  Remote Code Execution (RCE) (Authenticated)
| php/webapps/5[01;31m[K22[m[K25.txt

Cacti v1.2.[01;31m[K22[m[K - Remote Command Execution (RCE)
| php/webapps/51166.py

Cafelog b2 0.6 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K672.txt

Camiro-CMS_beta-0.1 - 'FCKeditor' Arbitrary File Upload
| php/webapps/1[01;31m[K22[m[K51.php

CamShot WebCam 2.6 Trial - Remote Buffer Overflow
| windows/remote/20[01;31m[K22[m[K4.txt

CANDID - '/image/view.php?image_id' Cross-Site Scripting
| php/webapps/34[01;31m[K22[m[K0.txt

Canon GP300 - Remote GET Denial of Service
| hardware/dos/[01;31m[K22[m[K876.txt

Captaris Infinite WebMail 3.61.5 - HTML Injection
| php/webapps/[01;31m[K22[m[K104.txt

Car Rental Project 1.0 - Remote Code Execution
| php/webapps/5[01;31m[K22[m[K43.py

CartWIZ 1.10 - 'searchresults.asp' Name Argument Cross-Site Scripting
| asp/webapps/255[01;31m[K22[m[K.txt

CascadianFAQ 4.1 - 'index.php' SQL Injection
| php/webapps/3[01;31m[K22[m[K7.txt

Casdoor 1.901.0 - Cross-Site Request Forgery (CSRF)
| go/webapps/5[01;31m[K22[m[K81.html

Caucho Technology Resin 1.2/1.3 - JavaBean Disclosure
| multiple/remote/207[01;31m[K22[m[K.txt

Cayman 3[01;31m[K22[m[K0-H DSL Router 1.0/GatorSurf 5.3 - Denial of
Service                                                 |
hardware/dos/19923.txt

CDRTools 2.0 - RSCSI Debug File Arbitrary Local File Manipulation
| linux/local/[01;31m[K22[m[K979.txt

CDRTools CDRecord 1.11/2.0 - Devname Format String
| linux/local/[01;31m[K22[m[K594.c

Cedric Email Reader 0.2/0.3 - Skin Configuration Script Remote File
Inclusion                                |
php/webapps/[01;31m[K22[m[K241.txt
```

Cedric Email Reader 0.4 - Global Configuration Script Remote File Inclusion |
php/webapps/[01;31m[K22[m[K242.txt

Celestial Software AbsoluteTelnet 2.0/2.11 - Title Bar Buffer Overflow
| windows/remote/[01;31m[K22[m[K[01;31m[K22[m[K9.pl

CenterIM 4.[01;31m[K22[m[K.3 - Remote Command Execution
| linux/remote/5283.txt

CentOS Web Panel 0.9.8.740 - Cross-Site Request Forgery / Cross-Site Scripting |
php/webapps/458[01;31m[K22[m[K.txt

Cerberus FTP Server 2.1 - Information Disclosure
| windows/remote/[01;31m[K22[m[K504.txt

Cerberus FTP Server 2.32 - Denial of Service
| windows/dos/14[01;31m[K22[m[K.c

Cerberus Helpdesk 2.x - 'Spellwin.php' Cross-Site Scripting
| php/webapps/29[01;31m[K22[m[K2.txt

CesarFTP 0.99 g - Remote 'Username' Buffer Overrun
| windows/dos/[01;31m[K22[m[K788.pl

CesarFTP 0.99 g - Remote CWD Denial of Service
| windows/dos/[01;31m[K22[m[K789.pl

cftp 0.12 - Banner Parsing Buffer Overflow
| freebsd/remote/[01;31m[K22[m[K890.pl

CH-CMS.ch 2 - Multiple Arbitrary File Upload Vulnerabilities
| php/webapps/339[01;31m[K22[m[K.txt

ChangshinSoft EZTrans Server - 'download.php' Directory Traversal
| php/webapps/[01;31m[K22[m[K886.txt

Check Point FW-1 Syslog Daemon - Unfiltered Escape Sequence
| hardware/remote/[01;31m[K22[m[K394.txt

CheckPoint/Sofaware Firewall - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K22[m[K493.txt

CHETCPASSWD 1.12 - Shadow File Disclosure
| cgi/webapps/[01;31m[K22[m[K111.pl

Chipmunk Pwngame - Multiple SQL Injections
| php/webapps/15[01;31m[K22[m[K3.txt

chipmunk topsites - Authentication Bypass / Cross-Site Scripting
| php/webapps/7[01;31m[K22[m[K7.txt

```
ChiTeX 6.1.2 - Local Privilege Escalation
| linux/local/[01;31m[K22[m[K452.sh

CHIYU IoT devices - 'Multiple' Cross-Site Scripting (XSS)
| cgi/webapps/499[01;31m[K22[m[K.txt

Church Edit - Blind SQL Injection
| php/webapps/3[01;31m[K22[m[K82.txt

Cisco Adaptive Security Appliance - Path Traversal (Metasploit)
| hardware/webapps/47[01;31m[K22[m[K0.rb

Cisco Adaptive Security Appliance Software 9.11 - Local File Inclusion
| hardware/webapps/487[01;31m[K22[m[K.txt

Cisco Aironet AP1x00 - GET Denial of Service
| hardware/dos/[01;31m[K22[m[K962.pl

Cisco Catalyst 2960 IOS 12.2(55)SE1 - 'ROCEM' Remote Code Execution
| hardware/remote/421[01;31m[K22[m[K.py

Cisco IOS 10/11/12 - UDP Echo Service Memory Disclosure
| hardware/dos/[01;31m[K22[m[K978.txt

Cisco IOS 11/12 - OSPF Neighbor Buffer Overflow
| hardware/remote/[01;31m[K22[m[K271.c

Cisco Small Business [01;31m[K22[m[K0 Series - Multiple Vulnerabilities
| hardware/remote/47442.py

Cisco Smart Software Manager On-Prem 8-20[01;31m[K22[m[K06 - Account
Takeover                                                  |
multiple/webapps/52155.py

Cisco WebEx Meeting Manager UCF - 'atucfobj.dll' ActiveX Remote Buffer
Overflow                                |
windows/remote/6[01;31m[K22[m[K0.html

CITSmart ITSM 9.1.2.[01;31m[K22[m[K - LDAP Injection
| java/webapps/49762.txt

CKEditor - 'posteddata.php' Cross-Site Scripting
| php/webapps/383[01;31m[K22[m[K.txt

ClanSphere 2011.3 - 'cs_lang' Cookie Local File Inclusion
| php/webapps/[01;31m[K22[m[K181.txt

ClassApps SelectSurvey.net - Multiple SQL Injections
| php/webapps/347[01;31m[K22[m[K.txt

Clean CMS 1.5 - Blind SQL Injection / Cross-Site Scripting
| php/webapps/7[01;31m[K22[m[K8.txt
```

```
Clearswift MAILsweeper 4.x - MIME Attachment Filter Bypass
| windows/remote/[01;31m[K22[m[K338.txt

Clever Internet ActiveX Suite 6.2 - Arbitrary File Download/Overwrite
| windows/remote/4[01;31m[K22[m[K6.html

CliServ Web Community 0.65 - 'cl_headers' Include
| php/webapps/[01;31m[K22[m[K57.txt

Cmaps v8.0 - SQL injection
| php/webapps/514[01;31m[K22[m[K.txt

CMS Frogss 0.4 - 'podpis' SQL Injection
| php/webapps/[01;31m[K22[m[K62.php

CMS MAXSITE Component Guestbook - Remote Command Execution
| php/webapps/73[01;31m[K22[m[K.pl

CMSQLite 1.3.2 - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K099.txt

cmsWorks 2.2 RC4 - 'FCKeditor' Arbitrary File Upload
| php/webapps/59[01;31m[K22[m[K.php

Cobalt RaQ4 - Administrative Interface Command Execution
| linux/remote/[01;31m[K22[m[K072.c

code-projects Online Exam Mastering System 1.0 - Reflected Cross-Site
Scripting (XSS)                       |
php/remote/5[01;31m[K22[m[K72.txt

CoffeeCup Software Password Wizard 4.0 - HTML Source Password Retrieval
| windows/local/[01;31m[K22[m[K329.c

ColdBookmarks 1.[01;31m[K22[m[K - SQL Injection
| windows/webapps/14933.txt

Comersus Cart 5.0 - HTTP Response Splitting
| asp/webapps/244[01;31m[K22[m[K.txt

CompactCMS 1.4.1 - Multiple Cross-Site Scripting Vulnerabilities (2)
| php/webapps/35[01;31m[K22[m[K8.txt

Compaq Client Management Agents 3.70/4.0 / Insight Management Agents
4.21 A/4.[01;31m[K22[m[K A/4.30 A / Intelligent Cl |
multiple/dos/19[01;31m[K22[m[K5.txt

Compaq Web-Based Management Agent - Access Violation Denial of Service
| windows/dos/[01;31m[K22[m[K823.txt

Compaq Web-Based Management Agent - Remote File Verification
| windows/remote/[01;31m[K22[m[K827.txt
```

```
Compaq Web-Based Management Agent - Remote Stack Overflow Denial of
Service                                    |
windows/dos/[01;31m[K22[m[K8[01;31m[K22[m[K.txt

compop.ca 3.5.3 - Arbitrary code Execution
| multiple/webapps/5[01;31m[K22[m[K57.txt

Computalynx CMail 2.3 - Web File Access
| windows/remote/19[01;31m[K22[m[K4.c

Computer Associates - Unicenter Asset Manager Stored Secret Data
Decryption                                 |
multiple/local/[01;31m[K22[m[K727.pl

Concrete CMS < 5.5.21 - Multiple Vulnerabilities
| php/webapps/37[01;31m[K22[m[K5.pl

Concrete5 CMS FlashUploader - Arbitrary '.SWF' File Upload
| php/webapps/37[01;31m[K22[m[K6.txt

ContaoCMS 2.10.1 - Cross-Site Scripting
| php/webapps/36[01;31m[K22[m[K5.txt

ContentNow 1.39 - 'pageid' SQL Injection
| php/webapps/28[01;31m[K22[m[K.pl

Coppermine Photo Gallery 1.0 - PHP Code Injection
| php/webapps/[01;31m[K22[m[K473.txt

coppermine photo Gallery 1.4.[01;31m[K22[m[K - Multiple Vulnerabilities
| php/webapps/8713.txt

Coppermine Photo Gallery 1.4.[01;31m[K22[m[K - SQL Injection
| php/webapps/8736.pl

Countly - Cross-Site Scripting
| php/webapps/45[01;31m[K22[m[K8.txt

course registration management system 2.1 - Multiple Vulnerabilities
| php/webapps/16[01;31m[K22[m[K2.txt

cPanel 5.0 - 'Guestbook.cgi' Remote Command Execution (1)
| cgi/webapps/[01;31m[K22[m[K260.c

cPanel 5.0 - 'Guestbook.cgi' Remote Command Execution (2)
| cgi/webapps/[01;31m[K22[m[K261.pl

cPanel 5.0 - 'Guestbook.cgi' Remote Command Execution (3)
| cgi/webapps/[01;31m[K22[m[K262.pl

cPanel 5.0 - 'Guestbook.cgi' Remote Command Execution (4)
| cgi/webapps/[01;31m[K22[m[K263.pl
```

cPanel 5.0 - 'Openwebmail' Local Privilege Escalation
| linux/local/[01;31m[K22[m[K265.pl

CPanel 5.0/5.3/6.x - Admin Interface HTML Injection
| php/webapps/[01;31m[K22[m[K874.txt

cPanel 5/6 / Formail-Clone - E-Mail Restriction Bypass
| php/webapps/[01;31m[K22[m[K693.txt

cPassMan 1.82 - Remote Command Execution
| php/webapps/185[01;31m[K22[m[K.php

Crob FTP Server 2.50.4 - Remote 'Username' Format String
| windows/dos/[01;31m[K22[m[K706.asm

CrushFTP 11.3.1 - Authentication Bypass
| multiple/remote/5[01;31m[K22[m[K95.py

Cryptocat 2.0.[01;31m[K22[m[K - Arbitrary Script Injection
| multiple/remote/38637.txt

CrystalPlayer 1.98 - '.mls' Local Buffer Overflow
| windows/local/4[01;31m[K22[m[K9.pl

CSF Firewall - Buffer Overflow (PoC)
| linux/dos/18[01;31m[K22[m[K5.c

CSO Lanifex Outreach Project Tool 0.946b - Request Origin Spoofing
| multiple/remote/[01;31m[K22[m[K179.pl

CubeCart 3.0.6 - Cross-Site Request Forgery (Add Admin)
| php/webapps/158[01;31m[K22[m[K.html

CUPS 1.1.x - Cupsd Request Method Denial of Service
| linux/dos/[01;31m[K22[m[K619.txt

CUPS 1.1.x - Negative Length HTTP Header
| linux/remote/[01;31m[K22[m[K106.txt

CuteNews 0.88 - 'comments.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K285.txt

CuteNews 0.88 - 'search.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K284.txt

CuteNews 0.88 - 'shownews.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K283.txt

CuteNews 1.4.0 - Shell Injection / Remote Command Execution
| php/webapps/1[01;31m[K22[m[K1.php

CutePHP CuteNews 1.3 - HTML Injection
| php/webapps/[01;31m[K22[m[K842.txt

```
CVS 1.11.x - Directory Request Double-Free Heap Corruption
| linux/remote/[01;31m[K22[m[K187.txt

CVSTrac 2.0.0 - Defacement Denial of Service
| cgi/dos/3[01;31m[K22[m[K3.pl

CyberGhost 6.0.4.[01;31m[K22[m[K05 - Local Privilege Escalation
| windows/local/41538.cs

CyberLink (Multiple Products) - File Project Handling Stack Buffer
Overflow (PoC)                          |
windows/dos/18[01;31m[K22[m[K0.py

CyberStrong EShop 4.2 - '20review.asp' SQL Injection
| asp/webapps/259[01;31m[K22[m[K.txt

CyBoards PHP Lite 1.21/1.25 - 'post.php' SQL Injection
| php/webapps/274[01;31m[K22[m[K.txt

Cybozu Products - 'id' Arbitrary File Retrieval
| cgi/webapps/[01;31m[K22[m[K66.txt

Cybuzu Garoon 2.1.0 - Multiple SQL Injections
| cgi/webapps/[01;31m[K22[m[K67.txt

Cyrus IMAPD 1.4/1.5.19/2.0.12/2.0.16/2.1.9/2.1.10 - Pre-Login Heap
Corruption                              |
linux/dos/[01;31m[K22[m[K061.txt

D-Bus Daemon < 1.2.4 - 'libdbus' Denial of Service
| multiple/dos/78[01;31m[K22[m[K.c

D-Forum 1 - 'footer' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K257.txt

D-Forum 1 - 'header' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K256.txt

D-Link AirPlus DI-614+ / DI-624 / DI-704 - DHCP Log HTML Injection
| hardware/remote/24[01;31m[K22[m[K6.txt

D-Link DI-614+ - IP Fragment Reassembly Denial of Service
| hardware/dos/[01;31m[K22[m[K440.c

D-Link DI-704P - Long URL Denial of Service
| hardware/dos/[01;31m[K22[m[K991.txt

D-Link DI-704P - Syslog.HTM Denial of Service
| hardware/dos/[01;31m[K22[m[K647.txt

D-Link DIR-645 - Multiple UPNP Vulnerabilities
| hardware/remote/387[01;31m[K22[m[K.txt
```

D-Link DNR-3[01;31m[K22[m[KL <=2.60B15 - Authenticated Remote Code Execution | hardware/remote/51046.txt

D-Link DSL-2760U-E1 - Persistent Cross-Site Scripting | hardware/webapps/338[01;31m[K22[m[K.sh

Daikin Security Gateway 14 - Remote Password Reset | multiple/local/5[01;31m[K22[m[K78.txt

Dasan Networks GPON ONT WiFi Router H64X Series - Privilege Escalation | hardware/webapps/423[01;31m[K22[m[K.txt

Datafeed Studio - 'patch.php' Remote File Inclusion | php/webapps/3[01;31m[K22[m[K26.txt

Datafeed Studio 1.6.2 - 'search.php' Cross-Site Scripting | php/webapps/3[01;31m[K22[m[K27.txt

dawa-pharma 1.0-20[01;31m[K22[m[K - Multiple-SQLi | php/webapps/51818.txt

DCP-Portal 5.0.1 - 'editor.php?Root' Remote File Inclusion | php/webapps/[01;31m[K22[m[K126.txt

DCP-Portal 5.0.1 - 'lib.php?Root' Remote File Inclusion | php/webapps/[01;31m[K22[m[K127.txt

DCP-Portal 5.3.1 - 'calendar.php' Cross-Site Scripting | php/webapps/[01;31m[K22[m[K387.txt

DDL CMS 1.0 - Multiple Remote File Inclusions | multiple/webapps/97[01;31m[K22[m[K.txt

DeepBurner 1.9.0.[01;31m[K22[m[K8 - Stack Buffer Overflow (SEH) (PoC) | windows/dos/8335.c

DeepBurner pro 1.9.0.[01;31m[K22[m[K8 - '.dbr' file Buffer Overflow (Universal) | windows/local/11315.c

Deerfield VisNetic WebSite 3.5.13.1 - Cross-Site Scripting | php/webapps/[01;31m[K22[m[K083.txt

Dell EMC iDRAC7/iDRAC8 2.52.52.52 - Remote Code Execution (RCE) | hardware/remote/5[01;31m[K22[m[K46.py

Dell EMC Networking PC5500 firmware versions 4.1.0.[01;31m[K22[m[K and Cisco Sx / SMB - Information Disclosure | hardware/remote/51248.py

Design4Online - 'Userpages2 Page.asp' SQL Injection | asp/webapps/296[01;31m[K22[m[K.txt

```
Desktop Orbiter 2.0 1 - Resource Exhaustion (Denial of Service)
| windows/dos/[01;31m[K22[m[K694.c

Dev-C++ 4.9.9.2 - '.CPP' File Parsing Local Stack Overflow (PoC)
| windows/dos/3[01;31m[K22[m[K9.py

Devalcms 1.4a - 'currentfile' Local File Inclusion
| php/webapps/58[01;31m[K22[m[K.txt

Devana - SQL Injection
| php/webapps/119[01;31m[K22[m[K.txt

Dew-NewPHPLinks 2.1b - 'index.php' SQL Injection
| php/webapps/161[01;31m[K22[m[K.txt

DieselScripts Diesel Paid Mail - 'Getad.php' Cross-Site Scripting
| php/webapps/284[01;31m[K22[m[K.txt

Digi Online Examination System 2.0 - Unrestricted Arbitrary File Upload
| php/webapps/35[01;31m[K22[m[K3.txt

DigiAffiliate 1.4 - 'id' SQL Injection
| asp/webapps/31[01;31m[K22[m[K.pl

Digital Attic Foundation CMS - 'id' SQL Injection
| php/webapps/363[01;31m[K22[m[K.txt

DigitalPersona 4.5.0.[01;31m[K22[m[K13 - 'DpHostW' Unquoted Service
Path                                                    |
windows/local/49008.txt

Disk Pulse Server 2.2.34 - 'GetServerInfo' Remote Buffer Overflow
(Metasploit)                                |
windows/remote/427[01;31m[K22[m[K.rb

DiskBoss v11.7.28 - Multiple Services Unquoted Service Path
| windows/local/490[01;31m[K22[m[K.txt

DIY-CMS 1.0 - Multiple Remote File Inclusions
| php/webapps/148[01;31m[K22[m[K.txt

dl_stats - Multiple Vulnerabilities
| php/webapps/1[01;31m[K22[m[K80.txt

Docebo Lms 4.0.4 - 'Messages' Remote Code Execution
| php/webapps/18[01;31m[K22[m[K4.php

Dokeos 1.x - 'viewtopic.php' SQL Injection
| php/webapps/276[01;31m[K22[m[K.txt

DokuWiki 2006-03-09b - 'dwpage.php' System Disclosure
| php/webapps/23[01;31m[K22[m[K.php
```

```
Dokuwiki 2018-04-[01;31m[K22[m[Kb - Username Enumeration
| php/webapps/47731.txt

Domain Group Network GooCMS 1.02 - 'index.php' Cross-Site Scripting
| php/webapps/3[01;31m[K22[m[K18.txt

DotBr 0.1 - 'Exec.php3' Remote Command Execution
| php/webapps/[01;31m[K22[m[K254.txt

DotBr 0.1 - 'System.php3' Remote Command Execution
| php/webapps/[01;31m[K22[m[K253.txt

dotProject 2.0 - '/modules/admin/vw_usr_roles.php?baseDir' Remote File
Inclusion                          |
php/webapps/27[01;31m[K22[m[K2.txt

dotProject 2.0 - '/modules/projects/gantt2.php?dPconfig[root_dir]'
Remote File Inclusion                   |
php/webapps/27[01;31m[K22[m[K0.txt

dotProject 2.0 - '/modules/projects/vw_files.php?dPconfig[root_dir]'
Remote File Inclusion                 |
php/webapps/27[01;31m[K22[m[K1.txt

dotProject 2.0 - '/modules/public/calendar.php?baseDir' Remote File
Inclusion                            |
php/webapps/27[01;31m[K22[m[K3.txt

dotProject 2.0 - '/modules/public/date_format.php?baseDir' Remote File
Inclusion                          |
php/webapps/27[01;31m[K22[m[K4.txt

dotProject 2.0 - '/modules/tasks/gantt.php?baseDir' Remote File
Inclusion                                  |
php/webapps/27[01;31m[K22[m[K5.txt

dotProject 2.1.6 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K708.txt

Dr.Web 4.x - Virus Scanner Folder Name Buffer Overflow (PoC)
| windows/dos/[01;31m[K22[m[K328.txt

DreamBox DM800 - Arbitrary File Download
| hardware/remote/174[01;31m[K22[m[K.txt

Drupal 11.x-dev - Full Path Disclosure
| php/webapps/5[01;31m[K22[m[K66.py

Drupal 4.1/4.2 - Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K940.txt

Drupal < 5.[01;31m[K22[m[K/6.16 - Multiple Vulnerabilities
| php/webapps/33706.txt
```

```
Drupal Module MiniorangeSAML 8.x-2.[01;31m[K22[m[K - Privilege
escalation                                                    |
php/webapps/50361.txt

DualDesk 20 - 'Proxy.exe' Denial of Service
| windows/dos/44[01;31m[K22[m[K2.txt

Dune 0.6.7 - GET Remote Buffer Overrun
| linux/remote/[01;31m[K22[m[K786.c

Dup Scout Enterprise 9.5.14 - GET Buffer Overflow (Metasploit)
| windows/remote/420[01;31m[K22[m[K.rb

Dyncms Release 6 - 'x_admindir' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K90.txt

DZcms 3.1 - SQL Injection
| php/webapps/77[01;31m[K22[m[K.txt

E-theni - Remote File Inclusion Command Execution
| php/webapps/[01;31m[K22[m[K293.txt

e107 < 0.75 - GLOBALS Overwrite Remote Code Execution
| php/webapps/[01;31m[K22[m[K68.php

e107 Website System 0.554 - HTML Injection
| php/webapps/[01;31m[K22[m[K958.txt

e107 Website System 0.555 - 'db.php' Information Disclosure
| php/webapps/[01;31m[K22[m[K956.txt

Easy File Sharing FTP Server 2.0 - 'PASS' Remote
| windows/remote/[01;31m[K22[m[K34.py

Easy File Sharing HTTP Server 7.2 - POST Buffer Overflow (Metasploit)
| windows/remote/4[01;31m[K22[m[K56.rb

Easy File Sharing Web Server 1.2 - Information Disclosure
| windows/remote/23[01;31m[K22[m[K2.txt

Easy File Sharing Web Server 7.2 - 'UserID' Remote Buffer Overflow (DEP
Bypass)                              |
windows/remote/445[01;31m[K22[m[K.py

Easy File Sharing Web Server 7.2 - Account Import Local Buffer Overflow
(SEH)                                |
windows/local/4[01;31m[K22[m[K67.py

Easy File Sharing Web Server 7.2 - GET 'PassWD' Remote Buffer Overflow
(SEH)                                 |
windows/remote/4[01;31m[K22[m[K61.py
```

Easy File Sharing Web Server 7.2 - Unrestricted File Upload
| windows/webapps/4[01;31m[K22[m[K68.py

Easy Karaokay Player 3.3.31 - '.wav' Integer Division by Zero
| windows/dos/304[01;31m[K22[m[K.py

Easy Software Products LPPassWd 1.1.[01;31m[K22[m[K - Resource Limit
Denial of Service |
windows/dos/25012.c

Easylogin Pro 1.3.0 - 'Encryptor.php' Unserialize Remote Code Execution
| php/remote/45[01;31m[K22[m[K7.php

EasyMail Objects 6.0.2.0 - 'emimap4.dll' ActiveX Control Remote Code
Execution |
windows/dos/33[01;31m[K22[m[K5.html

Easynet4u faq Host - 'faq.php' SQL Injection
| php/webapps/67[01;31m[K22[m[K.txt

ECI Telecom B-FOCuS Router 312+ - Unauthorized Access
| hardware/remote/260[01;31m[K22[m[K.txt

eclime 1.1 - Bypass / Create and Download Backup
| php/webapps/1[01;31m[K22[m[K79.txt

eDContainer 2.[01;31m[K22[m[K - Local File Inclusion
| php/webapps/7604.txt

Edgephp ClickBank Affiliate Marketplace Script - Multiple
Vulnerabilities |
php/webapps/143[01;31m[K22[m[K.txt

Edimax BR6[01;31m[K22[m[K8nS/BR6[01;31m[K22[m[K8nC - Multiple
Vulnerabilities
| hardware/webapps/38056.txt

eDonkey Clients 0.44/0.45 - Multiple Chat Dialog Resource Consumption
Vulnerabilities |
windows/dos/[01;31m[K22[m[K395.txt

eFiction < 2.0.7 - Remote Admin Authentication Bypass
| php/webapps/[01;31m[K22[m[K55.txt

eGroupWare 1.8.001.20110421 - Multiple Vulnerabilities
| php/webapps/173[01;31m[K22[m[K.txt

EHCP 0.[01;31m[K22[m[K.8 - Multiple Remote File Inclusions
| php/webapps/4671.txt

EJ3 BlackBook 1.0 - 'header.php' Multiple Cross-Site Scripting
Vulnerabilities |
php/webapps/317[01;31m[K22[m[K.txt

eLection 2.0 - 'id' SQL Injection
| php/webapps/481[01;31m[K22[m[K.txt

Electrasoft 32Bit FTP 9.49.1 - Client Long Server Banner Buffer
Overflow |
windows/dos/[01;31m[K22[m[K[01;31m[K22[m[K1.pl

Electronic Arts Battlefield 1942 1.2/1.3 - Remote Administration
Authentication Buffer Overflow |
windows/dos/[01;31m[K22[m[K290.c

Elm 2.3/2.4 - TERM Environment Variable Local Buffer Overrun
| linux/local/[01;31m[K22[m[K836.pl

Eltek SmartPack - Backdoor Account
| hardware/webapps/4[01;31m[K22[m[K52.txt

EMC NetWorker - Format String (Metasploit)
| windows/remote/[01;31m[K22[m[K525.rb

EMC xPression 4.5SP1 Patch 13 - 'model.jobHistoryId' SQL Injection
| multiple/webapps/434[01;31m[K22[m[K.txt

eMerge E3 1.00-06 - Arbitrary File Upload
| hardware/webapps/476[01;31m[K22[m[K.py

Empire CMS 3.7 - 'checklevel.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K39.txt

Emule 0.27b - Empty Nickname Chat Request Denial of Service
| windows/dos/[01;31m[K22[m[K420.txt

eNdonesia 8.4 - 'banners.php?click Action bid' SQL Injection
| php/webapps/30[01;31m[K22[m[K6.txt

eNdonesia 8.4 - 'mod.php?viewarticle Action artid' SQL Injection
| php/webapps/30[01;31m[K22[m[K5.txt

Endpoint Protector 4.0.4.0 - Multiple Vulnerabilities
| multiple/webapps/218[01;31m[K22[m[K.txt

Endpoint Protector 4.0.4.2 - Multiple Persistent Cross-Site Scripting
Vulnerabilities |
php/webapps/[01;31m[K22[m[K399.txt

Entertainment CMS - Local File Inclusion / Remote Command Execution
| php/webapps/4[01;31m[K22[m[K0.pl

Enthrallweb eHomes - 'compareHomes.asp' Multiple SQL Injections
| asp/webapps/291[01;31m[K22[m[K.txt

eoCMS 0.9.03 - Remote File Inclusion
| php/webapps/104[01;31m[K22[m[K.txt

Epic Games Unreal Engine 436 - Client Unreal URL Denial of Service
| multiple/dos/[01;31m[K22[m[K[01;31m[K22[m[K3.txt

Epic Games Unreal Engine 436 - URL Directory Traversal
| multiple/remote/[01;31m[K22[m[K[01;31m[K22[m[K4.txt

Equipment Inventory System 1.0 - 'multiple' Stored XSS
| php/webapps/497[01;31m[K22[m[K.txt

Ericsson HM[01;31m[K22[m[K0dp DSL Modem - World Accessible Web
Administration Interface |
hardware/remote/[01;31m[K22[m[K244.txt

Ero Auktion 2010 - 'news.php' SQL Injection
| php/webapps/115[01;31m[K22[m[K.txt

ERPGo SaaS 3.9 - CSV Injection
| php/webapps/51[01;31m[K22[m[K0.txt

ERPNext 14.82.1 - Account Takeover via Cross-Site Request Forgery
(CSRF) |
python/webapps/5[01;31m[K22[m[K83.txt

ES CmS 0.1 - SQL Injection
| php/webapps/[01;31m[K22[m[K907.txt

eScan Management Console 14.0.1400.[01;31m[K22[m[K81 - Cross Site
Scripting |
windows/webapps/51467.txt

eScan Management Console 14.0.1400.[01;31m[K22[m[K81 - SQL Injection
(Authenticated) |
windows/webapps/51466.txt

ESCPUtil 1.15.2 2 - Printer Name Local Buffer Overflow
| linux/local/[01;31m[K22[m[K190.txt

EServ 2.9x - Directory Indexing
| windows/remote/[01;31m[K22[m[K636.txt

eStore 1.0.1/1.0.2 - 'Settings.inc.php' Full Path Disclosure
| php/webapps/[01;31m[K22[m[K925.txt

Etano 1.20/1.[01;31m[K22[m[K - 'photo_search.php' Multiple Cross-Site
Scripting Vulnerabilities |
php/webapps/36899.txt

Etano 1.20/1.[01;31m[K22[m[K - 'photo_view.php?return' Cross-Site
Scripting |
php/webapps/36900.txt

```
Etano 1.20/1.[01;31m[K22[m[K - 'search.php' Multiple Cross-Site
Scripting Vulnerabilities                                  |
php/webapps/36898.txt

Ethercreative Logs 3.0.3 - Path Traversal
| multiple/webapps/5[01;31m[K22[m[K41.txt

EType EServ 1.9x - NNTP Remote Denial of Service
| windows/dos/[01;31m[K22[m[K124.pl

EType EServ 2.98/2.99/3.0 - Resource Exhaustion (Denial of Service) (1)
| windows/dos/[01;31m[K22[m[K585.pl

EType EServ 2.98/2.99/3.0 - Resource Exhaustion (Denial of Service) (2)
| windows/dos/[01;31m[K22[m[K586.c

EType EServ 2.9x - FTP Remote Denial of Service
| windows/dos/[01;31m[K22[m[K121.pl

EType EServ 2.9x - POP3 Remote Denial of Service
| windows/dos/[01;31m[K22[m[K1[01;31m[K22[m[K.pl

EType EServ 2.9x - SMTP Remote Denial of Service
| windows/dos/[01;31m[K22[m[K123.pl

EVA-Web 2.1.2 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                                        |
php/webapps/279[01;31m[K22[m[K.txt

Eventy CMS 1.8 Plus - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K684.txt

EveryBuddy 0.4.3 - Long Message Denial of Service
| multiple/dos/[01;31m[K22[m[K987.pl

eVestigator Forensic PenTester - Man In The Middle Remote Code
Execution                                          |
android/remote/4[01;31m[K22[m[K87.txt

ExBB 0.[01;31m[K22[m[K - Local/Remote File Inclusion
| php/webapps/5405.txt

ExBB Italiano 0.2 - exbb[home_path] Remote File Inclusion
| php/webapps/[01;31m[K22[m[K73.txt

Exceed 5.0/6.0/6.1/7.1/8.0 - Font Name Handler Buffer Overflow
| linux/remote/[01;31m[K22[m[K908.c

Exhibit Engine 1.[01;31m[K22[m[K - 'fetchsettings.php?toroot' Remote
File Inclusion                                          |
php/webapps/28873.txt
```

```
Exhibit Engine 1.[01;31m[K22[m[K - 'fstyles.php?toroot' Remote File
Inclusion                                              |
php/webapps/28874.txt

Exhibit Engine 1.[01;31m[K22[m[K - 'styles.php' Remote File Inclusion
| php/webapps/2850.txt

Exim Internet Mailer 3.35/3.36/4.10 - Format String
| linux/local/[01;31m[K22[m[K066.c

Expow 0.8 - 'autoindex.php?cfg_file' Remote File Inclusion
| php/webapps/37[01;31m[K22[m[K.txt

EyeLock Myris 3.3.2 - SDK Service Unquoted Service Path Privilege
Escalation                                    |
windows/local/40[01;31m[K22[m[K6.txt

EyeLock nano NXT 3.5 - Local File Disclosure
| php/webapps/40[01;31m[K22[m[K7.txt

EyeLock nano NXT 3.5 - Remote Code Execution
| php/webapps/40[01;31m[K22[m[K8.py

eyeos 1.9.0.2 - Persistent Cross-Site Scripting Using Image Files
| php/webapps/17[01;31m[K22[m[K0.txt

EZ Publish 2.2 - 'index.php' IMG Tag Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K607.txt

EZ Publish 2.2.7/3.0 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K22[m[K491.txt

EZ Publish 2.2.7/3.0 - Multiple Full Path Disclosure Vulnerabilities
| php/webapps/[01;31m[K22[m[K492.txt

EZ Publish 2.2.7/3.0 - site.ini Information Disclosure
| windows/remote/[01;31m[K22[m[K488.txt

EZ Server 1.0 - File Disclosure
| windows/remote/[01;31m[K22[m[K506.txt

EZ Server 1.0 - Long Argument Local Denial of Service
| linux/dos/[01;31m[K22[m[K446.txt

EZ Systems HTTPBench 1.1 - Information Disclosure
| php/webapps/[01;31m[K22[m[K009.txt

ezbounce 1.0/1.5 - Format String
| linux/remote/[01;31m[K22[m[K848.c

EZHomeTech EzServer 7.0 - Remote Heap Corruption
| windows/dos/[01;31m[K22[m[K006.txt
```

F5 BIG-IP 10.1.0 - Directory Traversal
| jsp/webapps/35[01;31m[K22[m[K2.txt

Fantastic News 2.1.3 - 'script_path' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K21.txt

FAQ Manager 1.2 - 'categorie.php' SQL Injection
| php/webapps/7[01;31m[K22[m[K4.txt

FAQ Manager 1.2 - 'header.php' Remote File Inclusion
| php/webapps/7[01;31m[K22[m[K9.txt

FAR-PHP 1.0 - 'index.php' Local File Inclusion
| php/webapps/3[01;31m[K22[m[K87.txt

Fastream NETFile Web Server 7.1.2 - 'HEAD' Denial of Service
| windows/dos/1[01;31m[K22[m[K0.pl

FCKEditor Core - 'FileManager test.html' Arbitrary File Upload (1)
| php/webapps/1[01;31m[K22[m[K54.txt

Fedora 21 setroubleshootd 3.2.[01;31m[K22[m[K - Local Privilege
Escalation |
linux/local/36564.txt

Feed CMS 1.07.03.19b - 'lang' Local File Inclusion
| php/webapps/74[01;31m[K22[m[K.txt

File 3.x - Local Stack Overflow Code Execution (1)
| unix/local/[01;31m[K22[m[K324.c

File 3.x - Local Stack Overflow Code Execution (2)
| unix/local/[01;31m[K22[m[K325.c

File 3.x - Utility Local Memory Allocation
| linux/local/[01;31m[K22[m[K326.c

FileCOPA FTP Server 5.01 - 'NOOP' Denial of Service
| windows/dos/33[01;31m[K22[m[K0.txt

FileRun < 2017.09.18 - SQL Injection
| php/webapps/429[01;31m[K22[m[K.py

FileSeek - CGI Script File Disclosure
| cgi/webapps/[01;31m[K22[m[K[01;31m[K22[m[K8.txt

FileSeek CGI Script - Remote Command Execution
| cgi/webapps/[01;31m[K22[m[K[01;31m[K22[m[K7.txt

FileZilla 2.2.15 - FTP Client Hard-Coded Cipher Key
| windows/dos/26[01;31m[K22[m[K0.c

FingerTec Fingerprint Reader - Remote Access and Remote Enrolment
| hardware/remote/39[01;31m[K22[m[K7.txt

FipsCMS 2.1 - 'neu.asp' SQL Injection
| asp/webapps/3[01;31m[K22[m[K55.txt

Fire Soft Board 2.0.1 - Persistent Cross-Site Scripting (Admin Panel)
| php/webapps/175[01;31m[K22[m[K.txt

Firebird 1.0 - GDS_Inet_Server Interbase Environment Variable Buffer
Overflow |
freebsd/local/[01;31m[K22[m[K580.c

Firefox ESR 115.11 - PDF.js Arbitrary JavaScript execution
| multiple/remote/5[01;31m[K22[m[K73.py

Firejail - Local Privilege Escalation
| linux/local/410[01;31m[K22[m[K.md

FlashChat 4.5.7 - 'aedating4CMS.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K93.txt

FlashFXP 1.4 - User Password Encryption
| windows/local/[01;31m[K22[m[K564.c

Flat Assembler 1.7.21 - Local Buffer Overflow
| linux/local/4[01;31m[K22[m[K65.py

Flex File Manager - Arbitrary File Upload
| php/webapps/1[01;31m[K22[m[K92.txt

Flex Timesheet - Authentication Bypass
| php/webapps/15[01;31m[K22[m[K0.txt

FlexCMS 2.5 - 'inc-core-admin-editor-previouscolorsjs.php' Cross-Site
Scripting |
php/webapps/3[01;31m[K22[m[K54.txt

Flexcustomer 0.0.6 - Admin Authentication Bypass / Possible PHP Code
Writing |
php/webapps/76[01;31m[K22[m[K.txt

FLIR AX8 1.46.16 - Remote Command Injection
| hardware/webapps/5[01;31m[K22[m[K40.py

FloosieTek FTGate 2.1 - Web File Access
| multiple/remote/19[01;31m[K22[m[K3.txt

FloosieTek FTGate PRO 1.[01;31m[K22[m[K - SMTP MAIL FROM Buffer
Overflow |
windows/dos/[01;31m[K22[m[K568.pl

```
FloosieTek FTGate PRO 1.[01;31m[K22[m[K - SMTP RCPT TO Buffer Overflow
| windows/dos/[01;31m[K22[m[K569.pl

FloosieTek FTGatePro 1.[01;31m[K22[m[K - Mail Server Cross-Site
Scripting                                                  |
windows/remote/23092.txt

FloosieTek FTGatePro 1.[01;31m[K22[m[K - Mail Server Full Path
Disclosure                                                 |
windows/remote/23091.txt

Fluig 1.7.0 - Path Traversal
| multiple/webapps/496[01;31m[K22[m[K.sh

FlyHelp - '.CHM' Local Buffer Overflow (PoC)
| windows/dos/9[01;31m[K22[m[K2.cpp

Folder Lock 5.9.5 - Weak Password Encryption Local Information
Disclosure                                  |
php/webapps/3[01;31m[K22[m[K81.cs

Fonality trixbox - 'mac' Remote Code Injection
| php/webapps/3[01;31m[K22[m[K63.txt

Fonality trixbox - SQL Injection
| php/webapps/3[01;31m[K22[m[K39.txt

Fool's Workshop Owl's Workshop 1.0 - 'multiplechoice/index.php'
Arbitrary File Access                       |
php/webapps/237[01;31m[K22[m[K.txt

Foreman Smart-Proxy - Remote Command Injection
| multiple/remote/39[01;31m[K22[m[K2.txt

FormatFactory 3.0.1 - Profile File Handling Buffer Overflow
| windows/local/[01;31m[K22[m[K851.py

FormMail-Clone - Cross-Site Scripting
| cgi/webapps/[01;31m[K22[m[K137.txt

Fortinet FortiClient 5.2.3 (Windows 10 x64 Post-Anniversary) - Local
Privilege Escalation                  | windows_x86-
64/local/417[01;31m[K22[m[K.c

Fortinet FortiOS_ FortiProxy_ and FortiSwitchManager 7.2.0 -
Authentication bypass                          |
windows/remote/5[01;31m[K22[m[K39.py

Fortinet Single Sign On - Stack Overflow
| windows/dos/364[01;31m[K22[m[K.txt

FoxCMS 1.2.5 - Remote Code Execution  (RCE)
| multiple/webapps/5[01;31m[K22[m[K67.bash
```

FoxPlayer 2.3.0 - '.m3u' Buffer Overflow
| windows/dos/15[01;31m[K22[m[K9.pl

Free Opener - Local Denial of Service
| windows/dos/18[01;31m[K22[m[K3.pl

FreeBSD - 'FGPE' Stack Clash (PoC)
| freebsd_x86/dos/4[01;31m[K22[m[K78.c

FreeBSD - 'FGPU' Stack Clash (PoC)
| freebsd_x86/dos/4[01;31m[K22[m[K77.c

FreeBSD - 'setrlimit' Stack Clash (PoC)
| freebsd_x86/dos/4[01;31m[K22[m[K79.c

FreeBSD - SCTP Remote NULL Ptr Dereference Denial of Service
| freebsd/dos/20[01;31m[K22[m[K6.c

FreeBSD 4.8 - 'realpath()' Off-by-One Buffer Overflow
| freebsd/remote/[01;31m[K22[m[K976.pl

Freefloat FTP Server - 'PUT' Remote Buffer Overflow
| windows/remote/[01;31m[K22[m[K351.py

Freefloat FTP Server - Arbitrary File Upload (Metasploit)
| windows/remote/23[01;31m[K22[m[K6.rb

FreeNews 2.1 - Include Undefined Variable Command Execution
| php/webapps/[01;31m[K22[m[K047.txt

FreePBX 2.11.0 - Remote Command Execution
| php/webapps/3[01;31m[K22[m[K14.pl

Freeware Advanced Audio Coder (FAAC) 1.28 - Denial of Service
| linux/dos/4[01;31m[K22[m[K07.txt

Freeway 1.4.1 - Multiple Input Validation Vulnerabilities
| php/webapps/3[01;31m[K22[m[K40.txt

Freeway 1.4.1.171 - '/english/account.php?language' Traversal Local
File Inclusion |
php/webapps/3[01;31m[K22[m[K59.txt

Freeway 1.4.1.171 - '/french/account_newsletters.php?language'
Traversal Local File Inclusion |
php/webapps/3[01;31m[K22[m[K64.txt

Freeway 1.4.1.171 -
'/includes/modules/faqdesk/faqdesk_article_require.php?language'
Traversal Local File | php/webapps/3[01;31m[K22[m[K65.txt

Freeway 1.4.1.171 -
'/includes/modules/newsdesk/newsdesk_article_require.php?language'
Traversal Local Fil | php/webapps/3[01;31m[K22[m[K66.txt

Freeway 1.4.1.171 - '/templates/Freeway/boxes/card1.php?language'
Traversal Local File Inclusion |
php/webapps/3[01;31m[K22[m[K67.txt

Freeway 1.4.1.171 - '/templates/Freeway/boxes/loginbox.php?language'
Traversal Local File Inclusion |
php/webapps/3[01;31m[K22[m[K68.txt

Freeway 1.4.1.171 - '/templates/Freeway/boxes/whos_online.php?language'
Traversal Local File Inclusion | php/webapps/3[01;31m[K22[m[K69.txt

Freeway 1.4.1.171 -
'/templates/Freeway/mainpage_modules/mainpage.php?language' Traversal
Local File Inclu | php/webapps/3[01;31m[K22[m[K70.txt

FreeWnn 1.1.1 - JServer Logging Option Data Corruption
| linux/local/[01;31m[K22[m[K775.txt

Friends in War Make or Break 1.3 - Authentication Bypass
| php/webapps/[01;31m[K22[m[K736.txt

friendsinwar FAQ Manager - 'view_faq.php?question' SQL Injection
| php/webapps/[01;31m[K22[m[K766.txt

friendsinwar FAQ Manager - SQL Injection / Authentication Bypass
| php/webapps/[01;31m[K22[m[K710.txt

Frisk F-Prot AntiVirus 3.12b - Command Line Scanner Buffer Overflow
| unix/remote/[01;31m[K22[m[K292.pl

FS Facebook Clone - 'token' SQL Injection
| php/webapps/43[01;31m[K22[m[K8.txt

FS IMDB Clone - 'id' SQL Injection
| php/webapps/43[01;31m[K22[m[K7.txt

FTLS Guestbook 1.1 - Script Injection
| php/webapps/[01;31m[K22[m[K202.txt

FTPGetter Professional 5.97.0.[01;31m[K22[m[K3 - Denial of Service
(PoC) |
windows/dos/47871.txt

Fujitsu Web-Based Admin View 2.1.2 - Directory Traversal
| linux/remote/3[01;31m[K22[m[K86.txt

FunkBoard 0.66 - 'register.php' Multiple Cross-Site Scripting
Vulnerabilities |
php/webapps/261[01;31m[K22[m[K.txt

```
Galeria Zdjec 3.0 - 'zd_numer.php' Local File Inclusion
| php/webapps/3[01;31m[K22[m[K5.pl

Gallery 1.2/1.3.x - Search Engine Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K961.txt

GameSpy 3D 2.62 - Packet Amplification Denial of Service
| linux/dos/[01;31m[K22[m[K183.c

Garage Management System 1.0 (categoriesName) - Stored XSS
| multiple/webapps/5[01;31m[K22[m[K38.txt

GDL 4.x - 'node' SQL Injection
| php/webapps/8[01;31m[K22[m[K8.txt

GeBlog 0.1 (Windows) - GLOBALS[tplname] Local File Inclusion
| php/webapps/35[01;31m[K22[m[K.pl

Geeklog 1.3.7 - 'comment.php?cid' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K165.txt

Geeklog 1.3.7 - 'Homepage User' HTML Injection
| php/webapps/[01;31m[K22[m[K166.txt

Geeklog 1.3.7 - 'profiles.php' Multiple Cross-Site Scripting
Vulnerabilities                                 |
php/webapps/[01;31m[K22[m[K163.txt

Geeklog 1.3.7 - 'users.php?uid' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K164.txt

Geeklog 1.3.x - (Authenticated) SQL Injection
| php/webapps/[01;31m[K22[m[K675.txt

GeoMoose < 2.9.2 - Directory Traversal
| php/webapps/418[01;31m[K22[m[K.txt

Gert Doering mgetty 1.1.19/1.1.20/1.1.21/1.[01;31m[K22[m[K.8 - Symbolic
Link Traversal                                    | unix/local/20179.txt

GestioIP 3.5.7 - Cross-Site Request Forgery (CSRF)
| multiple/remote/5[01;31m[K22[m[K00.txt

GestioIP 3.5.7 - Cross-Site Scripting (XSS)
| multiple/remote/5[01;31m[K22[m[K03.txt

GestioIP 3.5.7 - Reflected Cross-Site Scripting (Reflected XSS)
| multiple/remote/5[01;31m[K22[m[K02.txt

GestioIP 3.5.7 - Remote Command Execution (RCE)
| multiple/remote/5[01;31m[K22[m[K04.txt
```

GestioIP 3.5.7 - Stored Cross-Site Scripting (Stored XSS)
| multiple/remote/5[01;31m[K22[m[K01.txt

Geutebruck 5.02024 G-Cam/EFD-[01;31m[K22[m[K50 - 'simple_loglistjs.cgi'
Remote Command Execution (Metasploit) |
hardware/webapps/44957.rb

Geutebruck 5.02024 G-Cam/EFD-[01;31m[K22[m[K50 - 'testaction.cgi'
Remote Command Execution (Metasploit) |
hardware/webapps/41360.rb

Ghostscript 9.20 - 'Filename' Command Execution
| windows/local/41[01;31m[K22[m[K1.txt

Gitea 1.[01;31m[K22[m[K.0 - Stored XSS
| multiple/webapps/52077.txt

GitLab Community Edition (CE) 13.10.3 - 'Sign_Up' User Enumeration
| ruby/webapps/498[01;31m[K22[m[K.txt

GIU Gallery Image Upload 0.3.1 - 'category' SQL Injection
| php/webapps/456[01;31m[K22[m[K.txt

GKrellM Mailwatch Plugin 2.4.1/2.4.2 - From Header Remote Buffer
Overflow |
linux/remote/[01;31m[K22[m[K873.c

Gkrellmd 2.1 - Remote Buffer Overflow (1)
| freebsd/dos/[01;31m[K22[m[K831.pl

Gkrellmd 2.1 - Remote Buffer Overflow (2)
| freebsd/remote/[01;31m[K22[m[K832.pl

GlassFish Application Server - '/resourceNode/customResourceNew.jsf'
Multiple Cross-Site Scripting Vulnera |
multiple/remote/319[01;31m[K22[m[K.txt

gleamtech filevista/fileultimate 4.6 - Directory Traversal
| windows/webapps/[01;31m[K22[m[K972.txt

glFTPd 1.x/2.0 'ZIP' Plugins - Multiple Directory Traversal
Vulnerabilities |
linux/remote/251[01;31m[K22[m[K.txt

GlobalScape CuteFTP 5.0 - LIST Response Buffer Overflow
| windows/remote/[01;31m[K22[m[K184.pl

GlobalSunTech Access Point GL24[01;31m[K22[m[KAP-0T - Information
Disclosure |
hardware/remote/21983.c

GLPI 0.90.4 - SQL Injection
| php/webapps/4[01;31m[K22[m[K62.txt

GLPI 4.0.2 - Unauthenticated Local File Inclusion on Manageentities plugin |
php/webapps/51[01;31m[K22[m[K9.txt

Gnew 2013.1 - Multiple Vulnerabilities (1)
| php/webapps/275[01;31m[K22[m[K.txt

GNOME Evolution 2.[01;31m[K22[m[K.2 - 'html_engine_get_view_width()' Denial of Service |
linux/dos/31979.html

GNOME Eye Of Gnome 1.0.x/1.1.x/2.2 - Format String
| linux/local/[01;31m[K22[m[K376.txt

gnome_segv - Local Buffer Overflow
| linux/local/[01;31m[K22[m[K2.c

GNU AN - Command Line Option Local Buffer Overflow
| linux/local/[01;31m[K22[m[K861.c

GNU binutils - 'aarch64_ext_ldst_reglist' Buffer Overflow
| linux/dos/4[01;31m[K22[m[K04.txt

GNU binutils - 'bfd_get_string' Stack Buffer Overflow
| linux/dos/4[01;31m[K22[m[K00.txt

GNU binutils - 'decode_pseudodbg_assert_0' Buffer Overflow
| linux/dos/4[01;31m[K22[m[K01.txt

GNU binutils - 'ieee_object_p' Stack Buffer Overflow
| linux/dos/4[01;31m[K22[m[K02.txt

GNU binutils - 'print_insn_score16' Buffer Overflow
| linux/dos/4[01;31m[K22[m[K03.txt

GNU Chess 5.0 - Local Buffer Overflow
| linux/local/[01;31m[K22[m[K860.c

GNU Emacs [01;31m[K22[m[K.1 - Local Variable Handling Code Execution
| linux/remote/30736.txt

GNU GNATS 3.0 02 - PR-Edit Command Line Option Heap Corruption
| linux/dos/[01;31m[K22[m[K814.txt

GNU GNATS 3.113 - Environment Variable Buffer Overflow
| linux/local/[01;31m[K22[m[K815.c

GNU GNATS 3.113.1_6 - Queue-PR Database Command Line Option Buffer Overflow |
unix/local/[01;31m[K22[m[K939.pl

GNU Mailman 2.1 - 'email' Cross-Site Scripting
| cgi/webapps/[01;31m[K22[m[K198.txt

```
GNU Mailman 2.1 - Error Page Cross-Site Scripting
| cgi/webapps/[01;31m[K22[m[K199.txt

GNUPanel 0.3.5_R4 - Multiple Vulnerabilities
| php/webapps/3[01;31m[K22[m[K07.txt

GoAutoDial CE 3.3 - Authentication Bypass / Command Injection
(Metasploit)                                    |
unix/remote/4[01;31m[K22[m[K96.rb

GONiCUS System Administrator 1.0 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K279.txt

Google Android - libstagefright Integer Overflow Remote Code Execution
| android/remote/38[01;31m[K22[m[K6.py

Google Android 2.0 < 2.1 - Code Execution (Reverse Shell
10.0.2.2:[01;31m[K22[m[K[01;31m[K22[m[K/TCP)
| android/remote/15423.html

Google Chrome - MetaCharacter URI Obfuscation
| windows/dos/7[01;31m[K22[m[K6.html

Google Chrome - Out-of-Bounds Access in RegExp Stubs
| multiple/dos/4[01;31m[K22[m[K86.txt

Gordano NTMail 4.2 - Web File Access
| multiple/remote/19[01;31m[K22[m[K2.txt

Grafik CMS - '/admin.php' SQL Injection / Cross-Site Scripting
| php/webapps/34[01;31m[K22[m[K2.html

Grand Theft Auto III/Vice City Skin File v1.1 - Buffer Overflow
| windows/local/51[01;31m[K22[m[K3.py

Grassroots DICOM (GDCM) 2.6.0 and 2.6.1 -
ImageRegionReader::ReadIntoBuffer Buffer Overflow                |
linux/dos/39[01;31m[K22[m[K9.cpp

GreenCMS 2.3.0603 - Information Disclosure
| php/webapps/449[01;31m[K22[m[K.txt

Gretech GOM Encoder 1.0.0.11 - '.Subtitle' Buffer Overflow (PoC)
| windows/dos/8[01;31m[K22[m[K5.py

Grokability Snipe-IT 8.0.4 - Insecure Direct Object Reference (IDOR)
| php/webapps/5[01;31m[K22[m[K82.txt

Grundig Smart Inter@ctive 3.0 - Cross-Site Request Forgery
| hardware/webapps/450[01;31m[K22[m[K.txt

GS Real Estate Portal - Multiple SQL Injections
| php/webapps/71[01;31m[K22[m[K.txt
```

```
GTCatalog 0.8.16/0.9 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K317.txt

Guestbook 4.0 - Sensitive Information Disclosure
| cgi/webapps/[01;31m[K22[m[K482.txt

GuildFTPd 0.999.8 - 'CWD' Denial of Service
| windows/dos/[01;31m[K22[m[K790.txt

GuppY 2.4 - Remote File Access
| php/webapps/23[01;31m[K22[m[K0.txt

GuppY 4.5.16 - Remote Command Execution
| php/webapps/3[01;31m[K22[m[K1.php

H-Sphere 2.x - HTML Template Inclusion Cross-Site Scripting
| java/webapps/[01;31m[K22[m[K752.txt

H-Sphere WebShell 2.4 - Local Privilege Escalation
| linux/local/[01;31m[K22[m[K128.c

H-Sphere WebShell 2.4 - Remote Command Execution
| linux/remote/[01;31m[K22[m[K129.c

H2 Database - 'Alias' Arbitrary Code Execution
| java/local/444[01;31m[K22[m[K.py

Half-Life 1.1 Client - Server Message Format String
| windows/remote/[01;31m[K22[m[K142.c

Half-Life AdminMod 2.50 Plugin - Remote Format String
| linux/remote/[01;31m[K22[m[K141.c

Half-Life ClanMod 1.80/1.81 Plugin - Remote Format String
| multiple/remote/[01;31m[K22[m[K139.c

Half-Life StatsMe 2.6.x Plugin - CMD_ARGV Buffer Overflow
| multiple/remote/[01;31m[K22[m[K138.c

Half-Life StatsMe 2.6.x Plugin - MakeStats Format String
| multiple/remote/[01;31m[K22[m[K140.c

HappyMall E-Commerce Software 4.3/4.4 - 'Member_HTML.cgi' Command
Execution                                |
cgi/webapps/[01;31m[K22[m[K572.pl

HappyMall E-Commerce Software 4.3/4.4 - 'Normal_HTML.cgi' Command
Execution                                |
cgi/webapps/[01;31m[K22[m[K571.pl

Happymall E-Commerce Software 4.3/4.4 - 'Normal_HTML.cgi' Cross-Site
Scripting                               |
cgi/webapps/[01;31m[K22[m[K588.txt
```

Happymall E-Commerce Software 4.3/4.4 - 'Normal_HTML.cgi' File Disclosure |
cgi/webapps/[01;31m[K22[m[K592.txt

Hashicorp vagrant-vmware-fusion 4.0.23 - Local Privilege Escalation
| macos/local/43[01;31m[K22[m[K4.sh

Hashicorp vagrant-vmware-fusion 4.0.24 - Local Privilege Escalation
| macos/local/43[01;31m[K22[m[K3.sh

Hashicorp vagrant-vmware-fusion 5.0.0 - Local Privilege Escalation
| macos/local/43[01;31m[K22[m[K2.sh

Hashicorp vagrant-vmware-fusion 5.0.1 - Local Privilege Escalation
| macos/local/43[01;31m[K22[m[K0.sh

HeffnerCMS 1.[01;31m[K22[m[K - 'index.php' Local File Inclusion
| php/webapps/34608.txt

HM Software S to Infinity 3.0 - Multiple Vulnerabilities
| windows/local/200[01;31m[K22[m[K.txt

hMAilServer 4.4.1 - IMAP Command Remote Denial of Service
| windows/dos/3[01;31m[K22[m[K29.txt

hMAilServer 5.3.3 - IMAP Remote Crash (PoC)
| windows/dos/[01;31m[K22[m[K302.rb

Hobosworld HobSR - Multiple SQL Injections
| php/webapps/267[01;31m[K22[m[K.txt

HolaCMS 1.2.x/1.4.x Voting Module - Directory Traversal Remote File Corruption |
php/webapps/25[01;31m[K22[m[K2.html

Honestech VHS to DVD 3.0.30 Deluxe - Local Buffer Overflow (SEH)
| windows/local/150[01;31m[K22[m[K.py

HooToo Tripmate HT-TM01 2.000.0[01;31m[K22[m[K - Cross-Site Request Forgery |
hardware/webapps/38081.txt

Horde Groupware Webmail 5.2.[01;31m[K22[m[K - Stored XSS
| multiple/webapps/49769.py

Horde Groupware Webmail Edition 5.2.[01;31m[K22[m[K - PHAR Loading
| php/webapps/48210.py

Horde Groupware Webmail Edition 5.2.[01;31m[K22[m[K - PHP File Inclusion |
php/webapps/48209.py

```
Horde Groupware Webmail Edition 5.2.[01;31m[K22[m[K - Remote Code
Execution                                          |
php/webapps/48215.sh

Horde Webmail 5.2.[01;31m[K22[m[K - Multiple Vulnerabilities
| php/webapps/46903.txt

Hotfoon Dialer 4.0 - Buffer Overflow (PoC)
| multiple/dos/[01;31m[K22[m[K010.txt

HP Compaq Insight Management Agent 5.0 - Format String
| hardware/dos/[01;31m[K22[m[K983.txt

HP Instant Support 1.0.[01;31m[K22[m[K - 'HPISDataManager.dll
ExtractCab' ActiveX Control Buffer Overflow              |
windows/remote/31873.xml

HP Instant Support 1.0.[01;31m[K22[m[K - 'HPISDataManager.dll
RegistryString' Buffer Overflow                          |
windows/dos/31877.xml

HP Instant Support 1.0.[01;31m[K22[m[K - 'HPISDataManager.dll StartApp'
ActiveX Control Insecure Method                | windows/dos/31876.xml

HP Instant Support 1.0.[01;31m[K22[m[K - 'HPISDataManager.dll' ActiveX
Control Arbitrary File Creation                  |
windows/dos/31878.xml

HP Instant Support 1.0.[01;31m[K22[m[K - 'HPISDataManager.dll' ActiveX
Control Arbitrary File Delete                    |
windows/dos/31879.xml

HP Instant TopTools 5.0 - Remote Denial of Service
| windows/dos/[01;31m[K22[m[K447.txt

HP Intelligent Management Center UAM - Remote Buffer Overflow
(Metasploit)                                    |
windows/remote/[01;31m[K22[m[K432.rb

HP JetDirect Printer - SNMP JetAdmin Device Password Disclosure
| hardware/remote/[01;31m[K22[m[K319.txt

HP OfficeJet 4630/7110 MYM1FN2025AR/2117A - Stored Cross-Site Scripting
(XSS)                              |
hardware/webapps/50[01;31m[K22[m[K7.py

HP Operations Agent - Opcode 'coda.exe' 0x34 Buffer Overflow
(Metasploit)                                     |
windows/remote/[01;31m[K22[m[K306.rb

HP Operations Agent - Opcode 'coda.exe' 0x8c Buffer Overflow
(Metasploit)                                     |
windows/remote/[01;31m[K22[m[K305.rb
```

HP-UX 10.x - rs.F3000 Unauthorized Access
| hp-ux/local/[01;31m[K22[m[K248.sh

HP-UX 10.x - stmkfont Alternate Typeface Library Buffer Overflow (1)
| hp-ux/local/[01;31m[K22[m[K246.c

HP-UX 10.x - stmkfont Alternate Typeface Library Buffer Overflow (2)
| hp-ux/local/[01;31m[K22[m[K247.sh

HP-UX 10.x/11.x - RExec Remote 'Username' Flag Local Buffer Overrun
| hp-ux/dos/[01;31m[K22[m[K552.txt

HP-UX 11 RWrite - Buffer Overflow
| hp-ux/dos/[01;31m[K22[m[K561.txt

HP-UX FTPD 1.1.214.4 - 'REST' Memory Disclosure
| hp-ux/remote/[01;31m[K22[m[K733.c

HPE 1.0 - HPEinc Remote File Inclusion (2)
| php/webapps/[01;31m[K22[m[K40.txt

HPSystem Management Homepage (SMH) 2.1.12 - 'message.php' Cross-Site
Scripting |
php/webapps/3[01;31m[K22[m[K98.txt

HPUX 10.20/11 Wall Message - Local Buffer Overflow
| hp-ux/local/[01;31m[K22[m[K231.txt

HT Editor 2.0.20 - Local Buffer Overflow (ROP)
| linux/local/[01;31m[K22[m[K683.pl

HTMLToNuke - Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K896.txt

Huawei B315s-[01;31m[K22[m[K - Information Leak
| hardware/webapps/45971.txt

Huawei EchoLife HG520 - Remote Information Disclosure
| hardware/remote/1[01;31m[K22[m[K98.txt

Huawei EchoLife HG520c - Modem Reset (Denial of Service)
| hardware/dos/1[01;31m[K22[m[K97.txt

Huawei Technologies eSpace Meeting Service 1.0.0.23 - Local Privilege
Escalation |
windows/local/3[01;31m[K22[m[K05.txt

Hubstaff 1.6.14-61e5e[01;31m[K22[m[Ke - 'wow64log' DLL Search Order
Hijacking |
windows/local/51461.txt

Hudson 1.[01;31m[K22[m[K3 - 'q' Cross-Site Scripting
| php/webapps/32047.txt

Hugging Face Transformers MobileViTV2 4.41.1 - Remote Code Execution (RCE) | python/remote/5[01;31m[K22[m[K27.txt

Humax HG100R 2.0.6 - Backup File Download | hardware/webapps/4[01;31m[K22[m[K84.py

Hunk Companion Plugin 1.9.0 - Unauthenticated Plugin Installation | multiple/webapps/5[01;31m[K22[m[K59.py

Hyleos ChemView 1.9.5.1 - ActiveX Control Buffer Overflow (Metasploit) | windows/remote/114[01;31m[K22[m[K.rb

Iatek PortalApp 3.3/4.0 - 'login.asp' Multiple Cross-Site Scripting Vulnerabilities | asp/webapps/34[01;31m[K22[m[K1.txt

iBilling 3.7.0 - Persistent Cross-Site Scripting / Reflected Cross-Site Scripting | php/webapps/400[01;31m[K22[m[K.txt

IBM 1754 GCM 1.18.0.[01;31m[K22[m[K011 - Remote Command Execution | hardware/remote/27706.txt

IBM AIX 4.3.3/5.1/5.2 - 'libIM' Buffer Overflow | aix/dos/[01;31m[K22[m[K249.txt

IBM AIX 4.3.x/5.1 - 'LSMCODE' Environment Variable Local Buffer Overflow | aix/local/[01;31m[K22[m[K756.pl

IBM AIX eNetwork Firewall 3.2/3.3 - Insecure Temporary File Creation | aix/local/19[01;31m[K22[m[K9.txt

IBM Bladecenter Management Module - Denial of Service | hardware/dos/1[01;31m[K22[m[K52.txt

IBM DB2 - Shared Library Injection | unix/local/[01;31m[K22[m[K989.pl

IBM DB2 9.7/10.1/10.5/11.1 - Command Line Processor Buffer Overflow | multiple/dos/4[01;31m[K22[m[K60.py

IBM DB2 db2job - File Overwrite | unix/local/[01;31m[K22[m[K988.sh

IBM EGatherer 2.0 - ActiveX Control Dangerous Method | windows/remote/24[01;31m[K22[m[K0.html

IBM eGatherer 3.20.0284.0 - ActiveX Remote Code Execution (Metasploit) | windows/remote/[01;31m[K22[m[K76.pm

IBM GCM16/32 1.20.0.[01;31m[K22[m[K575 - Multiple Vulnerabilities | php/remote/34132.txt

IBM Remote Control Software 1.0 - Code Execution
| windows/local/19[01;31m[K22[m[K7.txt

IBM U2 UniVerse 10.0.0.9 - 'uvrestore' Buffer Overflow (PoC)
| unix/dos/[01;31m[K22[m[K918.txt

IBM U2 UniVerse 10.0.0.9 - UVADMSH Buffer Overflow
| unix/dos/[01;31m[K22[m[K920.txt

IBM UniVerse 10.0.0.9 - 'uvadmsh' Local Privilege Escalation
| unix/local/[01;31m[K22[m[K912.txt

IBM Websphere Application Server 3.0.2 Server Plugin - Denial of
Service |
multiple/dos/20[01;31m[K22[m[K9.txt

IBMi Navigator 7.5 - HTTP Security Token Bypass
| multiple/webapps/5[01;31m[K22[m[K10.txt

IBMi Navigator 7.5 - Server Side Request Forgery (SSRF)
| multiple/webapps/5[01;31m[K22[m[K12.txt

iCal 3.7 - HTTP Request Denial of Service
| windows/dos/[01;31m[K22[m[K117.txt

iCal 3.7 - Remote Buffer Overflow (PoC)
| windows/dos/[01;31m[K22[m[K118.txt

icblogger 2.0 - 'YID' SQL Injection
| asp/webapps/[01;31m[K22[m[K87.txt

IdealBB 1.4.9 - 'error.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K22[m[K992.txt

iDev Rentals 1.0 - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K735.txt

IDevSpot PHPLinkExchange 1.01/1.02 - 'index.php' Multiple Cross-Site
Scripting Vulnerabilities |
php/webapps/3[01;31m[K22[m[K30.txt

Ifenslave 0.0.7 - Argument Local Buffer Overflow (1)
| linux/local/[01;31m[K22[m[K643.pl

Ifenslave 0.0.7 - Argument Local Buffer Overflow (2)
| linux/local/[01;31m[K22[m[K644.c

Ifenslave 0.0.7 - Argument Local Buffer Overflow (3)
| linux/local/[01;31m[K22[m[K645.c

IglooFTP 0.6.1 - Banner Parsing Buffer Overflow
| freebsd/remote/[01;31m[K22[m[K891.pl

IglooFTP PRO 3.8 - Multiple Buffer Overflow Vulnerabilities (1)
| windows/remote/[01;31m[K22[m[K871.c

IglooFTP PRO 3.8 - Multiple Buffer Overflow Vulnerabilities (2)
| windows/remote/[01;31m[K22[m[K872.txt

iisCart2000 - Arbitrary File Upload
| asp/webapps/[01;31m[K22[m[K697.asp

IISPop 1.161/1.181 - Remote Buffer Overflow (Denial of Service) (PoC)
| windows/dos/[01;31m[K22[m[K019.pl

IISProtect 2.1/2.2 - Authentication Bypass
| windows/remote/[01;31m[K22[m[K631.txt

IISProtect 2.1/2.2 - Web Administration Interface SQL Injection
| asp/webapps/[01;31m[K22[m[K639.txt

IKE - Aggressive Mode Shared Secret Hash Leakage
| hardware/remote/[01;31m[K22[m[K532.txt

IKEView R60 - Local Buffer Overflow (SEH)
| windows/local/38[01;31m[K22[m[K0.py

IkonBoard 3.1 - Lang Cookie Arbitrary Command Execution (1)
| cgi/webapps/[01;31m[K22[m[K499.pl

IkonBoard 3.1 - Lang Cookie Arbitrary Command Execution (2)
| cgi/webapps/[01;31m[K22[m[K500.pl

ilchClan 1.0.5B - SQL Injection
| php/webapps/1[01;31m[K22[m[K56.txt

Image[01;31m[K22[m[K ActiveX 1.1.1 - Remote Buffer Overflow
| windows/remote/14321.html

ImageFolio 2.2x/3.0/3.1 - 'Admin.cgi' Directory Traversal
| cgi/webapps/[01;31m[K22[m[K743.txt

iMesh 7.1.0.x - 'IMWeb.dll 7.0.0.x' Remote Heap Overflow
| windows/remote/1[01;31m[K22[m[K44.txt

IMLib2 - Home Environment Variable Buffer Overflow
| linux/local/21[01;31m[K22[m[K6.c

In-link 2.3.4 - 'ADODB_DIR' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K95.txt

INCOGEN Bugport 1.x - Multiple SQL Injections
| php/webapps/270[01;31m[K22[m[K.txt

IndexScript 2.8 - 'cat_id' SQL Injection
| php/webapps/4[01;31m[K22[m[K5.txt

Infinity CGI Exploit Scanner 3.11 - Cross-Site Scripting
| cgi/webapps/[01;31m[K22[m[K770.txt

Infinity CGI Exploit Scanner 3.11 - Remote Command Execution
| cgi/webapps/[01;31m[K22[m[K772.txt

Info-ZIP UnZip 5.50 - Encoded Character Hostile Destination Path
| linux/remote/[01;31m[K22[m[K584.txt

Ingress Database Server 2.6 - Multiple Remote Vulnerabilities
| windows/dos/30[01;31m[K22[m[K4.py

Inktomi Traffic Server 4.0/5.x - Cross-Site Scripting
| linux/remote/[01;31m[K22[m[K601.txt

Inosoft VisiWin 7 20[01;31m[K22[m[K-2.1 - Insecure Folders Permissions
| windows/local/51682.txt

Inside Systems Mail 2.0 - 'error.php' Cross-Site Scripting
| php/webapps/29[01;31m[K22[m[K3.txt

InsOnSrv Asus InstantOn 2.3.1.1 - Unquoted Service Path Privilege
Escalation |
windows/local/405[01;31m[K22[m[K.txt

InstaBoard 1.3 - 'index.cfm' SQL Injection
| cfm/webapps/[01;31m[K22[m[K486.txt

InstantCMS 1.6 - PHP Remote Code Execution (Metasploit)
| php/remote/266[01;31m[K22[m[K.rb

INSTEON Hub [01;31m[K22[m[K42-[01;31m[K22[m[K2 - Lack of Web and API
Authentication |
hardware/webapps/27284.txt

Integramod Portal 2.0 rc2 - 'phpbb_root_path' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K56.txt

Integramod Portal 2.x - 'functions_portal.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K50.pl

Intel [01;31m[K22[m[K00BG 802.11 - Beacon frame Kernel Memory
Corruption |
multiple/dos/2949.c

Intel [01;31m[K22[m[K00BG 802.11 - disassociation packet Kernel Memory
Corruption |
windows/dos/3[01;31m[K22[m[K4.c

Intel Centrino ipw[01;31m[K22[m[K00BG - Wireless Driver Remote Buffer
Overflow (Metasploit) |
windows/remote/5461.rb

```
Intel Centrino ipw[01;31m[K22[m[K00BG - Wireless Driver Remote Overflow
| windows/remote/3158.c

IntelliTamper 2.07 - HTTP Header Remote Code Execution
| windows/remote/6[01;31m[K22[m[K7.c

IntelliTamper 2.07/2.08 - Remote Buffer Overflow (SEH)
| windows/remote/11[01;31m[K22[m[K0.py

Interact 2.2 - 'CONFIG[base_path]' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K18.txt

Interaction SIP Proxy 3.0 - Remote Heap Corruption Denial of Service
| multiple/dos/269[01;31m[K22[m[K.pl

Interbase 6.x - External Table File Verification
| multiple/remote/[01;31m[K22[m[K462.txt

Internet Security Systems ICECap Manager 2.0.23 - Default Username and
Password                              |
windows/remote/199[01;31m[K22[m[K.pl

InterSystems Cache 4.1.15/5.0.x - Insecure Default Permissions
| linux/local/[01;31m[K22[m[K847.txt

interuse Website Builder & design - 'index2.php' SQL Injection
| php/webapps/127[01;31m[K22[m[K.txt

Inventio Lite 4 - SQL Injection
| php/webapps/5[01;31m[K22[m[K63.py

InverseFlow 2.4 - Cross-Site Request Forgery (Add Admin)
| php/webapps/180[01;31m[K22[m[K.txt

Invision Board 1.1.1 - 'functions.php' SQL Injection
| php/webapps/[01;31m[K22[m[K461.txt

Invision Board 1.1.1 - 'ipchat.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K295.txt

Invision Community 5.0.6 - Remote Code Execution (RCE)
| multiple/remote/5[01;31m[K22[m[K94.php

Invision Power Board (IP.Board) 3.3.4 - 'Unserialize()' PHP Code
Execution                                |
php/webapps/[01;31m[K22[m[K398.php

Invision Power Board (IP.Board) 3.3.4 - 'Unserialize()' PHP Code
Execution (Metasploit)                   |
php/remote/[01;31m[K22[m[K686.rb

Invision Power Board (IP.Board) 3.3.4 - Unserialize Regex Bypass
| php/webapps/[01;31m[K22[m[K547.php
```

Iomega Home Media Network Hard Drive 2.038 < 2.061 - File-system Access
| hardware/remote/1[01;31m[K22[m[K65.txt

iOS iDocManager 1.0.0 - Directory Traversal
| ios/remote/16[01;31m[K22[m[K8.txt

iOS myDBLite 1.1.10 - Directory Traversal
| ios/remote/16[01;31m[K22[m[K9.txt

IP.Gallery - 'img' SQL Injection
| php/webapps/38[01;31m[K22[m[K9.txt

iParty Conferencing Server - Denial of Service
| multiple/dos/[01;31m[K22[m[K250.sh

iPlanet Messaging Server 5.0/5.1 - HTML Attachment Cross-Site Scripting
| multiple/remote/[01;31m[K22[m[K662.txt

IPNetSentryX / IPNetMonitorX - Unauthorized Network Reconnaissance
| linux/local/[01;31m[K22[m[K993.txt

IPSwitch IMail Server 2006 - SEARCH Remote Stack Overflow
| windows/remote/4[01;31m[K22[m[K3.pl

IPSwitch IMail Server 2006 9.10 - Subscribe Remote Overflow
| windows/remote/4[01;31m[K22[m[K8.pl

Ipswitch Instant Messaging 2.0.8.1 - Multiple Vulnerabilities
| windows/dos/311[01;31m[K22[m[K.txt

Ipswitch WS_FTP Home/Professional 8.0 - WS_FTP Client Format String
| windows/dos/3[01;31m[K22[m[K56.py

IPUX CS75[01;31m[K22[m[K/CS2330/CS2030 IP Camera - 'UltraHVCamX.ocx'
ActiveX Stack Buffer Overflow |
hardware/remote/354[01;31m[K22[m[K.txt

ircd-hybrid 7.0.1 / ircd-ratbox 1.5.1/2.0 - Socket Dequeuing Denial of
Service | linux/dos/24[01;31m[K22[m[K2.c

IrfanView - '.RLE' Image Decompression Buffer Overflow
| windows/dos/[01;31m[K22[m[K680.txt

IrfanView - '.TIF' Image Decompression Buffer Overflow
| windows/dos/[01;31m[K22[m[K681.txt

IRIX 5.x/6.x - MediaMail HOME Environment Variable Buffer Overflow
| irix/dos/[01;31m[K22[m[K638.txt

ISC BIND 8.3.x - OPT Record Large UDP Denial of Service
| linux/dos/[01;31m[K22[m[K011.c

```
ISDNRep 4.56 - Command Line Argument Local Buffer Overflow (1)
| linux/local/[01;31m[K22[m[K862.c

ISDNRep 4.56 - Command Line Argument Local Buffer Overflow (2)
| linux/local/[01;31m[K22[m[K863.c

iSO Air Files 2.6 - Directory Traversal
| hardware/remote/16[01;31m[K22[m[K6.txt

iSO Filer Lite 2.1.0 - Directory Traversal
| hardware/remote/16[01;31m[K22[m[K7.txt

ISPConfig - (Authenticated) Arbitrary PHP Code Execution (Metasploit)
| php/remote/293[01;31m[K22[m[K.rb

iSumsoft ZIP Password Refixer 3.1.1 - Buffer Overflow
| windows/local/44[01;31m[K22[m[K4.py

Itech Auction Script 6.49 - 'pid' SQL Injection
| php/webapps/41[01;31m[K22[m[K9.txt

Itech Inventory Management Software 3.77 - SQL Injection
| php/webapps/41[01;31m[K22[m[K6.txt

Itech News Portal Script 6.28 - 'sc' SQL Injection
| php/webapps/41[01;31m[K22[m[K8.txt

itMedia - Multiple SQL Injections
| php/webapps/3[01;31m[K22[m[K75.txt

Ivanti Connect Secure [01;31m[K22[m[K.7R2.5 - Remote Code Execution
(RCE)                                                    |
multiple/remote/5[01;31m[K22[m[K13.py

iXmail 0.2/0.3 - 'iXmail_NetAttach.php' File Deletion
| php/webapps/[01;31m[K22[m[K841.txt

iziContents RC6 - Remote Code Execution
| php/webapps/[01;31m[K22[m[K61.php

Jack De Winter WinSMTP 1.6 f/2.0 - Buffer Overflow
| windows/dos/20[01;31m[K22[m[K1.pl

JAD Java Decompiler 1.5.8e - Local Buffer Overflow (NX Enabled)
| linux/local/4[01;31m[K22[m[K55.py

Java Applet - JAX-WS Remote Code Execution (Metasploit)
| multiple/remote/[01;31m[K22[m[K657.rb

JAVA Web Start - Arbitrary Command-Line Injection
| multiple/remote/121[01;31m[K22[m[K.txt
```

```
JBC Explorer 7.20 - 'arbre.php' Cross-Site Scripting
| php/webapps/334[01;31m[K22[m[K.txt

jBilling 3.0.2 - Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K906.txt

JBoss 3.0.8/3.2.1 - HSQLDB Remote Command Injection
| multiple/remote/23[01;31m[K22[m[K1.txt

JCCorp URLShrink Free 1.3.1 - 'CreateURL.php' Remote File Inclusion
| php/webapps/297[01;31m[K22[m[K.txt

Jcow Social Networking Script 4.2 < 5.2 - Arbitrary Code Execution
(Metasploit)                              |
php/webapps/177[01;31m[K22[m[K.rb

Jedox 20[01;31m[K22[m[K.4.2 - Code Execution via RPC Interfaces
| php/webapps/51423.txt

Jedox 20[01;31m[K22[m[K.4.2 - Disclosure of Database Credentials via
Connection Checks                                    |
php/webapps/51429.txt

Jedox 20[01;31m[K22[m[K.4.2 - Remote Code Execution via Directory
Traversal                                              |
php/webapps/51424.txt

Jef Moine abcm2ps 3.7.20 - '.ABC' File Remote Buffer Overflow
| windows/remote/250[01;31m[K22[m[K.txt

Jira Scriptrunner 2.0.7 - Cross-Site Request Forgery / Remote Code
Execution (Metasploit)                   |
windows/remote/[01;31m[K22[m[K678.rb

Job Portal 3.1 - 'job_submit' SQL Injection
| php/webapps/466[01;31m[K22[m[K.txt

John Roy Pi3Web 2.0 For Windows - Remote Buffer Overflow
| windows/remote/21[01;31m[K22[m[K5.c

Joomla! / Mambo Component com_detail - 'id' SQL Injection
| php/webapps/31[01;31m[K22[m[K6.txt

Joomla! / Mambo Component com_profile - 'oid' SQL Injection
| php/webapps/31[01;31m[K22[m[K4.txt

Joomla! / Mambo Component Mod_Forum - 'PHPBB_Root.php' Remote File
Inclusion                                  |
php/webapps/30[01;31m[K22[m[K7.txt

Joomla! 1.0.9 - 'Weblinks' Blind SQL Injection
| php/webapps/19[01;31m[K22[m[K.php
```

```
Joomla! 1.5 - URL Redirecting
| php/webapps/147[01;31m[K22[m[K.txt

Joomla! 1.5.[01;31m[K22[m[K / 1.6.0 - 'com_mailto' Spam Mail Relay
| php/webapps/15979.txt

Joomla! 3.7 - SQL Injection
| php/remote/44[01;31m[K22[m[K7.php

Joomla! < 1.5.11 - Multiple Cross-Site Scripting / HTML Injection
Vulnerabilities                          |
php/webapps/330[01;31m[K22[m[K.txt

Joomla! Component Aardvertiser 2.1 - Blind SQL Injection
| php/webapps/149[01;31m[K22[m[K.txt

Joomla! Component Archery Scores 1.0.6 - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K82.txt

Joomla! Component Artlinks 1.0b4 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K09.txt

Joomla! Component BeeHeard 1.0 - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K39.txt

Joomla! Component Candle 1.0 - 'cid' SQL Injection
| php/webapps/5[01;31m[K22[m[K1.txt

Joomla! Component Community Builder Enhanced (CBE) 1.4.8/1.4.9/1.4.10 -
Local File Inclusion / Remote Code | php/webapps/15[01;31m[K22[m[K2.txt

Joomla! Component com_avosbillets - SQL Injection
| php/webapps/11[01;31m[K22[m[K3.txt

Joomla! Component com_biographies - SQL Injection
| php/webapps/11[01;31m[K22[m[K6.txt

Joomla! Component com_br - 'state_id' SQL Injection
| php/webapps/36[01;31m[K22[m[K1.txt

Joomla! Component com_collector - Arbitrary File Upload
| php/webapps/24[01;31m[K22[m[K8.txt

Joomla! Component com_commedia - 'task' SQL Injection
| php/webapps/[01;31m[K22[m[K152.txt

Joomla! Component com_fss 1.9.1.1447 - SQL Injection
| php/webapps/[01;31m[K22[m[K097.txt

Joomla! Component com_gameserver - SQL Injection
| php/webapps/11[01;31m[K22[m[K2.txt
```

Joomla! Component com_google - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K90.txt

Joomla! Component com_gurujibook - SQL Injection
| php/webapps/11[01;31m[K22[m[K5.txt

Joomla! Component com_hdflvplayer < 2.1.0.1 - SQL Injection
| multiple/webapps/35[01;31m[K22[m[K0.py

Joomla! Component com_icagenda - 'id' Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K004.txt

Joomla! Component com_jim 1.0.1 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K03.txt

Joomla! Component com_joomdocs - Cross-Site Scripting
| php/webapps/139[01;31m[K22[m[K.txt

Joomla! Component com_jr_tfb - 'Controller' Local File Inclusion
| php/webapps/359[01;31m[K22[m[K.txt

Joomla! Component com_kunena - 'search' SQL Injection
| php/webapps/[01;31m[K22[m[K153.pl

Joomla! Component com_manager 1.5.3 - 'id' SQL Injection
| php/webapps/1[01;31m[K22[m[K57.txt

Joomla! Component com_mygallery - 'cid' SQL Injection
| php/webapps/10[01;31m[K22[m[K7.txt

Joomla! Component com_pandafminigames - SQL Injection
| php/webapps/1[01;31m[K22[m[K70.txt

Joomla! Component com_rd_download - Local File Disclosure
| php/webapps/108[01;31m[K22[m[K.txt

Joomla! Component com_s5clanroster - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K31.txt

Joomla! Component com_sgicatalog 1.0 - 'id' SQL Injection
| php/webapps/36[01;31m[K22[m[K7.txt

Joomla! Component com_shop - 'id' SQL Injection
| php/webapps/36[01;31m[K22[m[K2.txt

Joomla! Component com_tag - 'tag' SQL Injection
| php/webapps/[01;31m[K22[m[K098.txt

Joomla! Component com_tree - 'key' SQL Injection
| php/webapps/36[01;31m[K22[m[K0.txt

Joomla! Component com_user - 'view' Open Redirection
| php/webapps/331[01;31m[K22[m[K.txt

Joomla! Component com_virtuemart 2.0.[01;31m[K22[m[Ka - SQL Injection
| php/webapps/27879.txt

Joomla! Component com_wgpicasa - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K30.txt

Joomla! Component Delicious Bookmarks 0.0.1 - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K37.txt

Joomla! Component Deluxe Blog Factory 1.1.2 - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K38.txt

Joomla! Component Fastball 1.1.0 < 1.2 - 'league' SQL Injection
| php/webapps/98[01;31m[K22[m[K.txt

Joomla! Component Gadget Factory 1.0.0 - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K85.txt

Joomla! Component GBU Facebook 1.0.5 - SQL Injection
| php/webapps/1[01;31m[K22[m[K99.txt

Joomla! Component iF surfALERT 1.2 - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K91.txt

Joomla! Component iNetLanka Contact Us Draw Root Map 1.1 - Local File
Inclusion |
php/webapps/1[01;31m[K22[m[K89.txt

Joomla! Component iNetLanka Multiple Map 1.0 - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K88.txt

Joomla! Component iNetLanka Multiple root 1.0 - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K87.txt

Joomla! Component Intellectual Property 1.5.3 - 'id' SQL Injection
| php/webapps/1[01;31m[K22[m[K46.txt

Joomla! Component JA Comment - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K36.txt

Joomla! Component JoltCard 1.2.1 - SQL Injection
| php/webapps/1[01;31m[K22[m[K69.txt

Joomla! Component JoomCRM 1.1.1 - SQL Injection
| php/webapps/461[01;31m[K22[m[K.txt

Joomla! Component JS Calendar 1.5.1 - Multiple Vulnerabilities
| php/webapps/15[01;31m[K22[m[K4.txt

Joomla! Component JS Jobs 1.0.5.8 - SQL Injection
| php/webapps/128[01;31m[K22[m[K.txt

Joomla! Component JS Support Ticket (com_jssupportticket) 1.1.6 - 'ticket.php' Arbitrary File Deletion | php/webapps/47[01;31m[K22[m[K3.txt

Joomla! Component JS Support Ticket (com_jssupportticket) 1.1.6 - 'ticketreply.php' SQL Injection | php/webapps/47[01;31m[K22[m[K2.txt

Joomla! Component Kochsuite 0.9.4 - Remote File Inclusion | php/webapps/[01;31m[K22[m[K15.txt

Joomla! Component Link Directory 1.0.3 - Remote File Inclusion | php/webapps/[01;31m[K22[m[K14.txt

Joomla! Component Love Factory 1.3.4 - Local File Inclusion | php/webapps/1[01;31m[K22[m[K35.txt

Joomla! Component Matamko 1.01 - Local File Inclusion | php/webapps/1[01;31m[K22[m[K86.txt

Joomla! Component Media Mall Factory 1.0.4 - Blind SQL Injection | php/webapps/1[01;31m[K22[m[K34.txt

Joomla! Component MediaLibrary Free 4.0.12 - SQL Injection | php/webapps/441[01;31m[K22[m[K.txt

Joomla! Component Mosets Tree 1.0 - Remote File Inclusion | php/webapps/[01;31m[K22[m[K05.txt

Joomla! Component MT Fire Eagle 1.2 - Local File Inclusion | php/webapps/1[01;31m[K22[m[K33.txt

Joomla! Component onisPetitions 2.5 - 'tag' SQL Injection | php/webapps/413[01;31m[K22[m[K.txt

Joomla! Component Photo Battle 1.0.1 - Local File Inclusion | php/webapps/1[01;31m[K22[m[K32.txt

Joomla! Component Poll 1.0.10 - Arbitrary Add Votes | php/webapps/[01;31m[K22[m[K19.php

Joomla! Component QPersonel 1.0.2 - SQL Injection | php/webapps/1[01;31m[K22[m[K00.txt

Joomla! Component Real Estate Property 3.1.[01;31m[K22[m[K-03 - 'aid' SQL Injection | php/webapps/12136.txt

Joomla! Component RokModule 1.1 - 'module' Blind SQL Injection | php/webapps/21[01;31m[K22[m[K1.txt

Joomla! Component Spider Catalog 1.1 - 'Product_ID' SQL Injection | php/webapps/[01;31m[K22[m[K403.txt

```
Joomla! Component vAccount 2.0.2 - 'vid' SQL Injection
| php/webapps/46[01;31m[K22[m[K6.txt

Joomla! Component vBizz 1.0.7 - Remote Code Execution
| php/webapps/46[01;31m[K22[m[K4.txt

Joomla! Component vBizz 1.0.7 - SQL Injection
| php/webapps/46[01;31m[K22[m[K3.txt

Joomla! Component VMap 1.9.6 - SQL Injection
| php/webapps/46[01;31m[K22[m[K9.txt

Joomla! Component vRestaurant 1.9.4 - SQL Injection
| php/webapps/46[01;31m[K22[m[K8.txt

Joomla! Component vReview 1.9.11 - SQL Injection
| php/webapps/46[01;31m[K22[m[K7.txt

Joomla! Component vWishlist 1.0.1 - SQL Injection
| php/webapps/46[01;31m[K22[m[K5.txt

Joomla! Component ZiMB Comment 0.8.1 - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K83.txt

Joomla! Component ZiMBCore 0.1 - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K84.txt

jQuery-File-Upload 9.[01;31m[K22[m[K.0 - Arbitrary File Upload
| php/webapps/45584.txt

Justice Guestbook 1.3 - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K444.txt

K Web CMS - 'sayfala.asp' SQL Injection
| asp/webapps/3[01;31m[K22[m[K78.txt

Kaspersky Anti-Virus File Server 8.0.3.297 - Multiple Vulnerabilities
| linux/webapps/4[01;31m[K22[m[K69.txt

Kasseler CMS 2 r1[01;31m[K22[m[K3 - Multiple Vulnerabilities
| php/webapps/26623.txt

Kayako SupportSuite 3.x - '/staff/index.php?customfieldlinkid' SQL
Injection                                |
php/webapps/3[01;31m[K22[m[K21.txt

Kayako SupportSuite 3.x - '/visitor/index.php?sessionid' Cross-Site
Scripting                               |
php/webapps/3[01;31m[K22[m[K19.txt

Kayako SupportSuite 3.x - 'index.php?filter' Cross-Site Scripting
| php/webapps/3[01;31m[K22[m[K20.txt
```

KDE Konqueror 3.0.3 - Malformed HTML Page Denial of Service
| linux/dos/[01;31m[K22[m[K560.txt

KDE Konqueror 3.5.x - ReplaceChild Denial of Service
| linux/dos/28[01;31m[K22[m[K0.txt

Kebi Academy 2001 - Input Validation
| cgi/webapps/[01;31m[K22[m[K377.txt

Kentico Xperience 13.0.178 - Cross Site Scripting (XSS)
| multiple/webapps/5[01;31m[K22[m[K90.py

Kerio MailServer 5.6.3 - Web Mail ADD_ACL Module Cross-Site Scripting
| cgi/webapps/[01;31m[K22[m[K799.txt

Kerio MailServer 5.6.3 - Web Mail DO_MAP Module Cross-Site Scripting
| cgi/webapps/[01;31m[K22[m[K804.txt

Kerio MailServer 5.6.3 add_acl Module - Overflow
| linux/dos/[01;31m[K22[m[K801.txt

Kerio MailServer 5.6.3 do_map Module - Overflow
| linux/dos/[01;31m[K22[m[K803.txt

Kerio MailServer 5.6.3 list Module - Overflow
| linux/dos/[01;31m[K22[m[K802.txt

Kerio MailServer 5.6.3 subscribe Module - Overflow
| linux/dos/[01;31m[K22[m[K800.txt

Kerio Personal Firewall 2.1.x - Remote Authentication Packet Buffer
Overflow (1) |
windows/dos/[01;31m[K22[m[K417.py

Kerio Personal Firewall 2.1.x - Remote Authentication Packet Buffer
Overflow (2) |
windows/remote/[01;31m[K22[m[K418.c

Key Focus KF Web Server 1.0.8 - Directory Traversal
| windows/remote/[01;31m[K22[m[K018.pl

KeystoneJS < 4.0.0-beta.7 - Cross-Site Request Forgery
| nodejs/webapps/439[01;31m[K22[m[K.html

KingSoft - 'UpdateOcx2.dll SetUninstallName()' Heap Overflow (PoC)
| windows/dos/5[01;31m[K22[m[K5.html

Kingsoft Office Writer 2012 8.1.0.3385 - '.wps' Local Buffer Overflow
(SEH) |
windows/local/299[01;31m[K22[m[K.py

KiTTY Portable 0.65.0.2p (Windows 8.1/10) - Local kitty.ini Overflow
| windows/local/391[01;31m[K22[m[K.py

KiviCare Clinic & Patient Management System (EHR) 3.6.4 - Unauthenticated SQL Injection | php/webapps/5[01;31m[K22[m[K65.py

KMplayer 2.9.4.1433 - '.srt' Local Buffer Overflow (PoC) | windows/dos/9[01;31m[K22[m[K0.pl

KMPlayer 3.3.0.33 - Multiple Vulnerabilities | windows/dos/[01;31m[K22[m[K467.txt

KnowledgeTree 3.5.2 Community Edition - Persistent Cross-Site Scripting | php/webapps/146[01;31m[K22[m[K.txt

KodExplorer 4.52 - Open Redirect | php/webapps/5[01;31m[K22[m[K45.txt

Koken CMS 0.[01;31m[K22[m[K.24 - Arbitrary File Upload (Authenticated) | php/webapps/48706.txt

kon2 - Local Buffer Overflow (1) | linux/local/[01;31m[K22[m[K719.pl

kon2 - Local Buffer Overflow (2) | linux/local/[01;31m[K22[m[K720.c

Konqueror 4.7.3 - Memory Corruption | linux/dos/[01;31m[K22[m[K406.txt

KosmosBlog 0.9.3 - SQL Injection / Cross-Site Scripting / Cross-Site Request Forgery | php/webapps/11[01;31m[K22[m[K4.txt

Kryn.cms 6.0 - Cross-Site Request Forgery / HTML Injection | multiple/webapps/34[01;31m[K22[m[K4.txt

Kshop 2.[01;31m[K22[m[K - 'kshop_search.php' Cross-Site Scripting | php/webapps/32190.txt

KubeLance 1.7.6 - Cross-Site Request Forgery (Add Admin) | php/webapps/113[01;31m[K22[m[K.txt

kusaba x 0.9.1 - Multiple Vulnerabilities | php/webapps/17[01;31m[K22[m[K1.txt

Kwintv - Local Buffer Overflow | linux/local/[01;31m[K22[m[K1.c

KwsPHP 1.0 sondages Module - SQL Injection | php/webapps/44[01;31m[K22[m[K.txt

LaCie 5big Network 2.2.8 - Command Injection | cgi/remote/43[01;31m[K22[m[K6.py

```
LAME 3.99.5 - 'III_dequantize_sample' Stack Buffer Overflow
| linux/dos/4[01;31m[K22[m[K59.txt

LAME 3.99.5 - 'II_step_one' Buffer Overflow
| linux/dos/4[01;31m[K22[m[K58.txt

LAN.FS Messenger 2.4 - Command Execution
| windows/remote/[01;31m[K22[m[K854.txt

Land Down Under 601/602/700/701/800/801 - 'events.php' HTML Injection
| php/webapps/26[01;31m[K22[m[K3.txt

LANDesk Lenovo ThinkManagement Suite 9.0.3 - Core Server Remote Code
Execution                              |
windows/remote/186[01;31m[K22[m[K.txt

Langflow 1.3.0 -  Remote Code Execution (RCE)
| multiple/remote/5[01;31m[K22[m[K62.txt

Lanifex DMO 2.3b - '_incMgr' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K80.pl

LaTeX2rtf 1.9.15 - Remote Buffer Overflow
| linux/remote/246[01;31m[K22[m[K.c

Laundry Booking Management System 1.0 - 'Multiple' Stored Cross-Site
Scripting (XSS)                        |
php/webapps/50[01;31m[K22[m[K0.txt

Lazarus Guestbook 1.[01;31m[K22[m[K - Multiple Vulnerabilities
| php/webapps/35605.txt

LBlog 1.05 - 'comments.asp' SQL Injection
| asp/webapps/[01;31m[K22[m[K30.txt

LBreakout2 2.x - Login Remote Format String
| linux/remote/[01;31m[K22[m[K830.c

LBT-T300-mini1 - Remote Buffer Overflow
| linux/remote/519[01;31m[K22[m[K.c

LedNews 0.7 Post Script - Code Injection
| cgi/webapps/[01;31m[K22[m[K777.txt

Leksbot 1.2 - Multiple Vulnerabilities
| linux/local/[01;31m[K22[m[K567.c

Lepide Auditor Suite - 'createdb()' Web Console Database Injection /
Remote Code Execution                  |
php/remote/4[01;31m[K22[m[K97.py

LG MRA58K - 'ASFParser::SetMetaData' Stack Overflow
| android/dos/4[01;31m[K22[m[K85.txt
```

```
Lgames LTris 1.0.1 - Local Memory Corruption
| freebsd/local/[01;31m[K22[m[K574.pl

Lib CGI 0.1 - Include Buffer Overflow
| unix/remote/[01;31m[K22[m[K049.c

LibHTTPD 1.2 - POST Buffer Overflow
| linux/remote/[01;31m[K22[m[K016.c

Libmodplug 0.8.8.2 - '.abc' Stack Buffer Overflow (PoC)
| linux/dos/17[01;31m[K22[m[K2.c

Libopt.a 3.1x - Error Logging Buffer Overflow (1)
| linux/dos/[01;31m[K22[m[K537.c

Libopt.a 3.1x - Error Logging Buffer Overflow (2)
| linux/local/[01;31m[K22[m[K538.pl

libpng 1.4.2 - Denial of Service
| multiple/dos/144[01;31m[K22[m[K.c

LibreOffice < 6.0.1 - '=WEBSERVICE' Remote Arbitrary File Disclosure
| linux/remote/440[01;31m[K22[m[K.md

LibTIFF - 'tif_dirwrite.c' Denial of Service
| linux/dos/4[01;31m[K22[m[K99.txt

LibTIFF pal2rgb 4.0.9 - Heap Buffer Overflow
| linux/dos/433[01;31m[K22[m[K.txt

libvirt - 'virConnectListAllInterfaces' Method Denial of Service
| linux/dos/386[01;31m[K22[m[K.txt

Light HTTPd 0.1 - 'GET' Buffer Overflow (1)
| linux/remote/[01;31m[K22[m[K012.c

Light HTTPd 0.1 - 'GET' Buffer Overflow (2)
| linux/remote/[01;31m[K22[m[K013.c

LightNEasy 3.1.x - Multiple Vulnerabilities
| php/webapps/123[01;31m[K22[m[K.txt

Lighttpd 1.4.15 - Multiple Code Execution / Denial of Service /
Information Disclosure Vulnerabilities     |
windows/remote/303[01;31m[K22[m[K.rb

lighttpd 1.4.31 - Denial of Service (PoC)
| linux/dos/[01;31m[K22[m[K902.sh

Linkspider 1.08 - Multiple Remote File Inclusions
| php/webapps/3[01;31m[K22[m[K17.txt
```

Linksys BEFVP4 - SNMP Community String Information Disclosure
| hardware/remote/[01;31m[K22[m[K480.txt

Linksys Devices 1.42/1.43 - 'GET' Buffer Overflow (PoC)
| hardware/dos/[01;31m[K22[m[K062.py

Linksys WVC54GCA 1.00R[01;31m[K22[m[K/1.00R24 (Wireless-G) -
'adm/file.cgi' Multiple Directory Traversal Vulnerabilitie |
hardware/remote/32954.txt

Linksys WVC54GCA 1.00R[01;31m[K22[m[K/1.00R24 (Wireless-G) - Multiple
Cross-Site Scripting Vulnerabilities |
hardware/remote/32955.js

Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 /
Fedora [01;31m[K22[m[K/25 / CentOS 7.3.1611) - 'ldso_ | linux_x86-
64/local/4[01;31m[K22[m[K75.c

Linux Kernel (Debian 7/8/9/10 / Fedora 23/24/25 / CentOS
5.3/5.11/6.0/6.8/7.2.1511) - 'ldso_hwcap Stack Cl |
linux_x86/local/4[01;31m[K22[m[K74.c

Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora
23/24/25) - 'ldso_dynamic Stack Clash' L |
linux_x86/local/4[01;31m[K22[m[K76.c

Linux Kernel - 'espfix64' Nested NMIs Interrupting Privilege Escalation
| linux_x86-64/local/377[01;31m[K22[m[K.c

Linux Kernel - 'offset2lib' Stack Clash
| linux_x86/local/4[01;31m[K22[m[K73.c

Linux Kernel 2.0.x/2.2.x/2.4.x (FreeBSD 4.x) - Network Device Driver
Frame Padding Information Disclosure |
bsd/remote/[01;31m[K22[m[K131.pl

Linux Kernel 2.2 - 'mmap()' Local Denial of Service
| linux/dos/[01;31m[K22[m[K105.c

Linux Kernel 2.2 - Predictable TCP Initial Sequence Number
| linux/remote/195[01;31m[K22[m[K.txt

Linux Kernel 2.2.x/2.4.x - '/proc' Filesystem Information Disclosure
| linux/local/[01;31m[K22[m[K813.c

Linux Kernel 2.2.x/2.4.x - I/O System Call File Existence
| linux/local/[01;31m[K22[m[K458.c

Linux Kernel 2.2.x/2.4.x - Privileged Process Hijacking Privilege
Escalation (1) |
linux/local/[01;31m[K22[m[K362.c

Linux Kernel 2.2.x/2.4.x - Privileged Process Hijacking Privilege Escalation (2) | linux/local/[01;31m[K22[m[K363.c

Linux Kernel 2.2/2.4 - Deep Symbolic Link Denial of Service | linux/dos/211[01;31m[K22[m[K.sh

Linux Kernel 2.4 - SUID 'execve()' System Call Race Condition Executable File Read | linux/local/[01;31m[K22[m[K840.c

Linux Kernel 2.4.[01;31m[K22[m[K - 'do_brk()' Local Privilege Escalation (1) | linux/local/129.asm

Linux Kernel 2.4.[01;31m[K22[m[K - 'do_brk()' Local Privilege Escalation (2) | linux/local/131.c

Linux Kernel 2.4.[01;31m[K22[m[K-28/2.6.9 - 'igmp.c' Local Denial of Service | linux/dos/686.c

Linux Kernel 2.6.10 - File Lock Local Denial of Service | linux/dos/253[01;31m[K22[m[K.c

Linux Kernel 2.6.[01;31m[K22[m[K - IPv6 Hop-By-Hop Header Remote Denial of Service | linux/dos/30902.c

Linux Kernel 2.6.[01;31m[K22[m[K < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (SUID | linux/local/40616.c

Linux Kernel 2.6.[01;31m[K22[m[K < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Me | linux/local/40847.cpp

Linux Kernel 2.6.[01;31m[K22[m[K < 3.9 - 'Dirty COW PTRACE_POKEDATA' Race Condition (Write Access Method) | linux/local/40838.c

Linux Kernel 2.6.[01;31m[K22[m[K < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd | linux/local/40839.c

Linux Kernel 2.6.[01;31m[K22[m[K < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Method) | linux/local/40611.c

Linux Kernel 2.6.31 - 'perf_counter_open()' Local Buffer Overflow | linux/dos/33[01;31m[K22[m[K8.txt

Linux Kernel 2.6.31.4 - 'unix_stream_connect()' Local Denial of Service | linux/dos/100[01;31m[K22[m[K.c

```
Linux Kernel 2.6.37 - Unix Sockets Local Denial of Service
| linux/dos/156[01;31m[K22[m[K.c

Linux Kernel 2.6.x - 'pipe.c' Local Privilege Escalation (2)
| linux/local/333[01;31m[K22[m[K.c

Linux Kernel 3.10.0-[01;31m[K22[m[K9.x (CentOS / RHEL 7.1) -
'iowarrior' Driver Crash (PoC)                                  |
linux/dos/39556.txt

Linux Kernel 3.10.0-[01;31m[K22[m[K9.x (CentOS / RHEL 7.1) - 'snd-usb-
audio' Crash (PoC)                                | linux/dos/39555.txt

Linux Kernel 3.x (Ubuntu 14.04 / Mint 17.3 / Fedora [01;31m[K22[m[K) -
Double-free usb-midi SMEP Privilege Escalation   |
linux/local/41999.txt

Linux Kernel 4.8.0-[01;31m[K22[m[K/3.10.0-327 (Ubuntu 16.10 / RedHat) -
'keyctl' Null Pointer Dereference               | linux/dos/40762.c

Linux Kernel < 2.6.[01;31m[K22[m[K - 'ftruncate()'/'open()' Local
Privilege Escalation                                    |
linux/local/6851.c

Linux PAM 0.77 - Pam_Wheel Module 'getlogin() Username' Spoofing
Privilege Escalation                        |
linux/local/[01;31m[K22[m[K781.txt

Linux-ATM LES 2.4 - Command Line Argument Buffer Overflow
| linux/local/[01;31m[K22[m[K540.c

List Site Pro 2.0 - User Database Delimiter Injection
| multiple/remote/[01;31m[K22[m[K201.txt

ListProc 8.2.9 - Catmail ULISTPROC_UMASK Buffer Overflow
| freebsd/local/[01;31m[K22[m[K573.pl

LiveCart 1.1.1 - 'id' Blind SQL Injection
| php/webapps/54[01;31m[K22[m[K.pl

Logitech Media Server 7.9.0 - 'favorites' Cross-Site Scripting
| multiple/webapps/431[01;31m[K22[m[K.txt

LokiCMS 0.3.3 - Arbitrary File Delete
| php/webapps/55[01;31m[K22[m[K.txt

Lonerunner Zeroo HTTP Server 1.5 - Remote Buffer Overflow
| linux/remote/[01;31m[K22[m[K021.sh

LoveCMS 1.6.2 Final - Arbitrary File Delete
| php/webapps/70[01;31m[K22[m[K.txt
```

```
LPRng (RedHat 7.0) - 'lpd' Format String
| linux/remote/[01;31m[K22[m[K7.c

LPRng 3.6.[01;31m[K22[m[K/23/24 - Remote Command Execution
| linux/remote/[01;31m[K22[m[K6.c

LuxCal 3.2.2 - Cross-Site Request Forgery / Blind SQL Injection
| php/webapps/3[01;31m[K22[m[K11.txt

Lynx 2.8.x - Command Line URL CRLF Injection
| linux/remote/217[01;31m[K22[m[K.pl

M-TECH P-Synch 6.2.5 - 'nph-psa.exe?css' Cross-Site Scripting
| windows/remote/[01;31m[K22[m[K677.txt

M-TECH P-Synch 6.2.5 - 'nph-psa.exe?css' Remote File Inclusion
| cgi/webapps/[01;31m[K22[m[K689.txt

M-TECH P-Synch 6.2.5 - 'nph-psf.exe?css' Cross-Site Scripting
| windows/remote/[01;31m[K22[m[K676.txt

M-TECH P-Synch 6.2.5 - 'nph-psf.exe?css' Remote File Inclusion
| cgi/webapps/[01;31m[K22[m[K688.txt

M-TECH P-Synch 6.2.5 - Full Path Disclosure
| windows/remote/[01;31m[K22[m[K674.txt

Mabry Software HTTPServer/X 1.0 0.047 - File Disclosure
| windows/remote/[01;31m[K22[m[K892.txt

Macromedia ColdFusion MX 6.0 - Error Message Full Path Disclosure
| cfm/webapps/[01;31m[K22[m[K544.txt

Macromedia ColdFusion MX 6.0 - Remote Development Service File
Disclosure                                  |
multiple/remote/[01;31m[K22[m[K867.pl

Macromedia Dreamweaver MX 6.0 - PHP User Authentication Suite Cross-
Site Scripting                          |
php/webapps/[01;31m[K22[m[K986.txt

Macromedia Flash 6.0.47.0 - SWRemote Heap Corruption
| windows/remote/[01;31m[K22[m[K0[01;31m[K22[m[K.txt

Macromedia Flash 9 - IE Plugin Remote Crash (Denial of Service)
| windows/dos/[01;31m[K22[m[K08.html

Maelstrom Player 3.0.x - Argument Buffer Overflow (1)
| linux/local/[01;31m[K22[m[K616.pl

Maelstrom Player 3.0.x - Argument Buffer Overflow (2)
| linux/local/[01;31m[K22[m[K617.c
```

Maelstrom Server 3.0.x - Argument Buffer Overflow (1)
| freebsd/local/[01;31m[K22[m[K613.pl

Maelstrom Server 3.0.x - Argument Buffer Overflow (2)
| freebsd/local/[01;31m[K22[m[K614.c

Maelstrom Server 3.0.x - Argument Buffer Overflow (3)
| freebsd/local/[01;31m[K22[m[K615.c

Magic Photo Storage Website -
'/user/change_catalog_template.php?_config[site_path]' Remote File
Inclusion | php/webapps/294[01;31m[K22[m[K.txt

Magic Uploader Mini - Arbitrary File Upload
| php/webapps/1[01;31m[K22[m[K26.txt

Magic Winmail Server 2.3 USER POP3 - Command Format String
| windows/remote/[01;31m[K22[m[K635.c

Magneto Net Resource ActiveX 4.0.0.5 - 'NetConnectionEnum' Universal
| windows/remote/1[01;31m[K22[m[K48.html

Magneto Net Resource ActiveX 4.0.0.5 - 'NetFileClose' Universal
| windows/remote/1[01;31m[K22[m[K47.html

Magneto Net Resource ActiveX 4.0.0.5 - 'NetShareEnum' Universal
| windows/remote/1[01;31m[K22[m[K50.html

MagnetoSoft DNS 4.0.0.9 - ActiveX DNSLookupHostWithServer (PoC)
| windows/dos/1[01;31m[K22[m[K01.html

MagnetoSoft ICMP 4.0.0.18 - ActiveX AddDestinationEntry Buffer Overflow
| windows/remote/1[01;31m[K22[m[K02.html

MagnetoSoft NetworkResources - ActiveX NetConnectionEnum Overwrite
(SEH) (PoC) |
windows/dos/1[01;31m[K22[m[K08.html

MagnetoSoft NetworkResources 4.0.0.5 - ActiveX NetFileClose Overwrite
(SEH) (PoC) |
windows/dos/1[01;31m[K22[m[K06.html

MagnetoSoft NetworkResources 4.0.0.5 - ActiveX NetSessionDel (PoC)
| windows/dos/1[01;31m[K22[m[K05.html

MagnetoSoft NetworkResources 4.0.0.5 - ActiveX NetShareEnum Overwrite
(SEH) (PoC) |
windows/dos/1[01;31m[K22[m[K07.html

MagnetoSoft SNTP 4.0.0.7 - ActiveX SntpGetReply Buffer Overflow
| windows/remote/1[01;31m[K22[m[K03.html

MagnetoSoft SNTP 4.0.0.7 - ActiveX SntpSendRequest Crash (PoC)
| windows/dos/1[01;31m[K22[m[K04.html

MailEnable 1.501x - Email Server Buffer Overflow
| windows/remote/[01;31m[K22[m[K023.c

MailGust 1.9 - Board Takeover (SQL Injection)
| php/webapps/1[01;31m[K22[m[K7.php

Mailtraq 2.1.0.1302 - Remote Format String SMTP Resource Consumption
| windows/dos/[01;31m[K22[m[K780.txt

Mailtraq 2.1.0.1302 - User Password Encoding
| windows/local/[01;31m[K22[m[K779.pl

Mailtraq 2.2 - 'Browse.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K22[m[K730.txt

Mailtraq 2.2 - Webmail Utility Full Path Disclosure
| asp/webapps/[01;31m[K22[m[K731.txt

Malwarebytes Anti-Exploit 1.03.1.1[01;31m[K22[m[K0/1.04.1.1012 - Out-of-Bounds Read Denial of Service | windows/dos/35842.c

Malwarebytes Anti-Malware < 2.0.3 / Anti-Exploit < 1.03.1.1[01;31m[K22[m[K0 - Update Code Execution (Metasploit) | windows/local/41701.rb

Mambo Component 'com_a6mambocredits' 1.0.0 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K07.txt

Mambo Component 'com_phpshop' 1.2 RC2b - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K06.txt

Mambo Component bigAPE-Backup 1.1 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K25.txt

Mambo Component com_lurm_constructor 0.6b - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K[01;31m[K22[m[K.txt

Mambo Component cropimage 1.0 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K17.txt

Mambo Component eWriting 1.2.1 - 'cat' SQL Injection
| php/webapps/5[01;31m[K22[m[K6.txt

Mambo Component ExtCalendar 2.0 - Remote File Inclusion
| php/webapps/20[01;31m[K22[m[K.txt

Mambo Component mambelfish 1.1 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K02.txt

```
Mambo Component MamboWiki 0.9.6 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K13.txt

Mambo Component pollxt 1.[01;31m[K22[m[K.07 - Remote File Inclusion
| php/webapps/2029.txt

Mambo Open Source 4.6.2 -
'/administrator/popups/index3pop.php?mosConfig_sitename' Cross-Site
Scripting    | php/webapps/3[01;31m[K22[m[K52.txt

Mambo Open Source 4.6.2 - '/mambots/editors/mostlyce/'
PHP/connector.php?Query String Cross-Site Scripting |
php/webapps/3[01;31m[K22[m[K53.txt

Mambo Site Server 4.0.10 - 'index.php' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K382.txt

Mambo Site Server 4.0.11 - 'PHPInfo.php' Information Disclosure
| php/webapps/[01;31m[K22[m[K086.txt

Mambo Site Server 4.0.11 - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K087.txt

Mambo Site Server 4.0.12 RC2 - Cookie Validation
| php/webapps/[01;31m[K22[m[K281.php

Man 1.5.1 - Catalog File Format String
| linux/local/[01;31m[K22[m[K729.c

Man Command - -H Flag Local Buffer Overflow
| linux/local/298[01;31m[K22[m[K.c

Man Program 1.5 - Unsafe Return Value Command Execution
| linux/local/[01;31m[K22[m[K344.txt

ManageEngin AMP 4.3.0 - File-path-traversal
| multiple/webapps/51[01;31m[K22[m[K2.txt

ManageEngine Application Manager 14.2 - Privilege Escalation / Remote
Command Execution (Metasploit)       |
multiple/remote/47[01;31m[K22[m[K8.rb

ManageEngine Desktop Central - Java Deserialization (Metasploit)
| multiple/remote/48[01;31m[K22[m[K4.rb

ManageEngine OpManager - Remote Code Execution (Metasploit)
| java/remote/38[01;31m[K22[m[K1.rb

ManageEngine OpManager 12.4x - Privilege Escalation / Remote Command
Execution (Metasploit)               |
multiple/remote/47[01;31m[K22[m[K7.rb
```

```
ManageEngine OpManager 12.4x - Unauthenticated Remote Command Execution
(Metasploit)                        |
multiple/remote/47[01;31m[K22[m[K9.rb

ManageEngine Security Manager Plus 5.5 build 5505 - Directory Traversal
| multiple/webapps/[01;31m[K22[m[K092.py

ManageEngine Security Manager Plus 5.5 build 5505 - Remote Root/SYSTEM
SQL Injection                        |
multiple/remote/[01;31m[K22[m[K093.py

ManageEngine Security Manager Plus 5.5 build 5505 - Remote SYSTEM SQL
Injection (Metasploit)               |
windows/remote/[01;31m[K22[m[K094.rb

ManageEngine Security Manager Plus 5.5 build 5505 - SQL Injection
(Metasploit)                             |
multiple/remote/[01;31m[K22[m[K304.rb

ManageEngine ServiceDesk 8.0 - Multiple Vulnerabilities
| windows/webapps/[01;31m[K22[m[K879.txt

ManageEngine Support Center Plus 7908 - Multiple Vulnerabilities
| jsp/webapps/[01;31m[K22[m[K040.txt

ManageEngine SupportCenter Plus 7.90 - Multiple Vulnerabilities
| multiple/webapps/373[01;31m[K22[m[K.txt

ManDB Utility 2.3/2.4 - Local Buffer Overflow
| linux/local/[01;31m[K22[m[K971.txt

Mandrake 6.1/7.0/7.1 - '/perl' HTTP Directory Disclosure
| linux/remote/20[01;31m[K22[m[K0.txt

Mantis Bug Tracker 0.x/1.0 - 'manage_user_page.php?sort' Cross-Site
Scripting                            |
php/webapps/27[01;31m[K22[m[K9.txt

Mantis Bug Tracker 0.x/1.0 - 'view_all_set.php' Multiple Cross-Site
Scripting Vulnerabilities            |
php/webapps/27[01;31m[K22[m[K8.txt

MatterDaddy Market 1.1 - 'login.php' Cross-Site Scripting
| php/webapps/3[01;31m[K22[m[K99.txt

MAXcms 3.11.20b - Multiple Remote File Inclusions
| php/webapps/93[01;31m[K22[m[K.txt

MAXdev MD-Pro 1.0.73 - Arbitrary File Upload
| php/webapps/26[01;31m[K22[m[K5.txt

MAXdev MD-Pro 1.0.73 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/26[01;31m[K22[m[K6.txt
```

```
Maxthon3 - about:history XCS Trusted Zone Code Execution (Metasploit)
| windows/remote/23[01;31m[K22[m[K5.rb

Maxwebportal 1.30 - 'search.asp?Search' Cross-Site Scripting
| asp/webapps/[01;31m[K22[m[K746.txt

Maxwebportal 1.30 - Remote Database Disclosure
| asp/webapps/[01;31m[K22[m[K747.txt

MCCS (Multi-Computer Control Systems) Command - Denial of Service
| windows/dos/1[01;31m[K22[m[K2.pl

mcrypt 2.5.8 - Local Stack Overflow
| linux/local/[01;31m[K22[m[K928.pl

mcrypt 2.6.8 - Stack Buffer Overflow (PoC)
| linux/dos/[01;31m[K22[m[K938.py

MDaemon POP3 Server < 9.06 - 'USER' Remote Buffer Overflow (PoC)
| windows/dos/[01;31m[K22[m[K45.pl

MDaemon WebAdmin 2.0.x - SQL Injection
| windows/webapps/10[01;31m[K22[m[K5.txt

MDG Web Server 4D 3.6 - HTTP Command Buffer Overflow
| windows/remote/[01;31m[K22[m[K556.c

ME Download System 1.3 - 'header.php' Remote File Inclusion
| php/webapps/21[01;31m[K22[m[K.txt

MediaWiki 1.[01;31m[K22[m[K.1 PdfHandler - Remote Code Execution
| multiple/webapps/31329.txt

Meet#Web 0.8 - 'ManagerResource.class.php?root_path' Remote File
Inclusion                                 |
php/webapps/3[01;31m[K22[m[K32.txt

Meet#Web 0.8 - 'ManagerRightsResource.class.php?root_path' Remote File
Inclusion                               |
php/webapps/3[01;31m[K22[m[K33.txt

Meet#Web 0.8 - 'modules.php?root_path' Remote File Inclusion
| php/webapps/3[01;31m[K22[m[K31.txt

Meet#Web 0.8 - 'RegForm.class.php?root_path' Remote File Inclusion
| php/webapps/3[01;31m[K22[m[K34.txt

Meet#Web 0.8 - 'RegResource.class.php?root_path' Remote File Inclusion
| php/webapps/3[01;31m[K22[m[K35.txt

Meet#Web 0.8 - 'RegRightsResource.class.php?root_path' Remote File
Inclusion                                   |
php/webapps/3[01;31m[K22[m[K36.txt
```

```
Mega File Hosting Script 1.2 - 'emaillinks.php' Cross-Site Scripting
| php/webapps/33[01;31m[K22[m[K6.txt

MegaBook 1.1/2.0/2.1 - Multiple HTML Injection Vulnerabilities
| cgi/webapps/[01;31m[K22[m[K843.txt

MegaBook 2.0/2.1 - 'Admin.cgi?EntryID' Cross-Site Scripting
| cgi/webapps/256[01;31m[K22[m[K.txt

MegaBrowser 0.3 - HTTP Directory Traversal
| windows/remote/[01;31m[K22[m[K723.txt

Mercury/32 Mail Server 4.01a (Pegasus) - IMAP Buffer Overflow
| windows/remote/1[01;31m[K22[m[K3.c

MercuryBoard 1.1.4 - 'User-Agent' SQL Injection
| php/webapps/[01;31m[K22[m[K47.php

Mereo 1.8.0 - GET Remote Denial of Service
| windows/dos/87[01;31m[K22[m[K.py

Mersive Solstice 2.8.0 - Remote Code Execution
| android/webapps/477[01;31m[K22[m[K.py

Meta Search Engine Script - 'url' Local File Disclosure
| php/webapps/9[01;31m[K22[m[K7.txt

Meteocontrol WEB'log - Admin Password Disclosure (Metasploit)
| multiple/webapps/398[01;31m[K22[m[K.rb

Meteor FTP Server 1.2/1.5 - USER Memory Corruption
| windows/dos/[01;31m[K22[m[K999.pl

methane IRCd 0.1.1 - Remote Format String
| linux/dos/[01;31m[K22[m[K839.c

Methodus 3 Web Server - File Disclosure
| windows/remote/[01;31m[K22[m[K769.txt

Metyus Okul Yonetim 1.0 - 'Sistemi Uye_giris_islem.asp' SQL Injection
| asp/webapps/29[01;31m[K22[m[K0.html

Mhonarc 2.5.x - Mail Header HTML Injection
| linux/remote/[01;31m[K22[m[K026.txt

Michael Kohn Ringtone Tools 2.[01;31m[K22[m[K - '.EMelody' File Remote
Buffer Overflow                                  |
linux/remote/25015.txt

Microchip TimeProvider 4100 Grandmaster (Data plot modules) 2.4.6 - SQL
Injection                          |
hardware/remote/521[01;31m[K22[m[K.NA
```

```
MicroP 0.1.1.1600 - '.mppl' Local Stack Buffer Overflow
| windows/local/3[01;31m[K22[m[K61.rb

Micropoint ProActive Denfense 'Mp110013.sys' 1.3.10123.0 - Local
Privilege Escalation                      |
windows/local/1[01;31m[K22[m[K13.c

Microsoft 'Shlwapi.dll' 6.0.2800.1106 - Malformed HTML Form Tag Denial
of Service                           |
windows/dos/[01;31m[K22[m[K518.html

Microsoft - NTLM Hash Disclosure Spoofing (library-ms)
| windows/local/5[01;31m[K22[m[K80.txt

Microsoft ActiveSync 3.5 - Null Pointer Dereference Denial of Service
| windows/dos/[01;31m[K22[m[K390.c

Microsoft BizTalk Server 2000/2002 DTA - 'RawCustomSearchField.asp' SQL
Injection                          | asp/webapps/[01;31m[K22[m[K555.txt

Microsoft BizTalk Server 2000/2002 DTA - 'rawdocdata.asp' SQL Injection
| asp/webapps/[01;31m[K22[m[K554.txt

Microsoft BizTalk Server 2002 - HTTP Receiver Buffer Overflow
| windows/dos/[01;31m[K22[m[K553.txt

Microsoft Class Package Export Tool 5.0.2752 - 'Clspack.exe' Local
Buffer Overflow (PoC)                   |
windows/dos/288[01;31m[K22[m[K.txt

Microsoft Edge - 'CssParser::RecordProperty' Type Confusion
| windows/dos/4[01;31m[K22[m[K46.html

Microsoft Edge Chakra - 'AppendLeftOverItemsFromEndSegment' Out-of-
Bounds Read                              |
windows/dos/435[01;31m[K22[m[K.js

Microsoft Excel - Axis Properties Record Parsing Buffer Overflow (PoC)
(MS11-02)                          | windows/dos/17[01;31m[K22[m[K7.py

Microsoft Excel 2007 - WriteAV Crash (PoC)
| windows/dos/[01;31m[K22[m[K591.txt

Microsoft Excel 2010 - Crash (PoC) (1)
| windows/dos/[01;31m[K22[m[K330.txt

Microsoft Exchange 2019 15.2.[01;31m[K22[m[K1.12 - Authenticated Remote
Code Execution                                  |
windows/remote/48153.py

Microsoft Host Integration Server 8.5.4[01;31m[K22[m[K4.0 - Denial of
Service                                          |
windows/dos/17159.txt
```

```
Microsoft IIS - ISAPI 'nsiislog.dll' ISAPI POST Overflow (MS03-
0[01;31m[K22[m[K) (Metasploit)                              |
windows/remote/16355.rb

Microsoft IIS 4.0 / Microsoft JET 3.5/3.5.1 Database Engine - VBA
| multiple/dos/19[01;31m[K22[m[K8.pl

Microsoft IIS 5.0 (Windows XP/2000/NT 4.0) - WebDAV 'ntdll.dll' Remote
Buffer Overflow (1)                  |
windows/remote/[01;31m[K22[m[K365.pl

Microsoft IIS 5.0 (Windows XP/2000/NT 4.0) - WebDAV 'ntdll.dll' Remote
Buffer Overflow (2)                  |
windows/remote/[01;31m[K22[m[K366.c

Microsoft IIS 5.0 (Windows XP/2000/NT 4.0) - WebDAV 'ntdll.dll' Remote
Buffer Overflow (3)                  |
windows/remote/[01;31m[K22[m[K367.txt

Microsoft IIS 5.0 (Windows XP/2000/NT 4.0) - WebDAV 'ntdll.dll' Remote
Buffer Overflow (4)                  |
windows/remote/[01;31m[K22[m[K368.txt

Microsoft IIS 5.0 - User Existence Disclosure (1)
| windows/remote/[01;31m[K22[m[K562.pl

Microsoft IIS 5.0 - User Existence Disclosure (2)
| windows/remote/[01;31m[K22[m[K563.pl

Microsoft IIS 5.0 - WebDAV PROPFIND / SEARCH Method Denial of Service
| windows/dos/[01;31m[K22[m[K670.c

Microsoft Internet Explorer - 'wshom.ocx' (Run) ActiveX Code Execution
(Add Admin)                          |
windows/local/11[01;31m[K22[m[K9.txt

Microsoft Internet Explorer - COALineDashStyleArray Unsafe Memory
Access (MS12-0[01;31m[K22[m[K) (Metasploit)           |
windows/remote/29858.rb

Microsoft Internet Explorer - MSHTML Findtext Processing
| windows/dos/151[01;31m[K22[m[K.html

Microsoft Internet Explorer - Multiple COM Object Color Property Denial
of Service Vulnerabilities         | windows/dos/[01;31m[K22[m[K38.html

Microsoft Internet Explorer 11 - OLE Automation Array Remote Code
Execution (1)                              |
windows/remote/35[01;31m[K22[m[K9.html

Microsoft Internet Explorer 5 - Classic Mode FTP Client Cross Domain
Scripting                            |
windows/remote/[01;31m[K22[m[K728.txt
```

Microsoft Internet Explorer 5 - Custom HTTP Error HTML Injection
| windows/remote/[01;31m[K22[m[K784.txt

Microsoft Internet Explorer 5 - OBJECT Tag Buffer Overflow
| windows/remote/[01;31m[K22[m[K726.txt

Microsoft Internet Explorer 5 - Remote 'URLMON.dll' Remote Buffer
Overflow |
windows/remote/[01;31m[K22[m[K530.pl

Microsoft Internet Explorer 5 - ShowHelp Arbitrary Command Execution
| windows/remote/[01;31m[K22[m[K[01;31m[K22[m[K6.txt

Microsoft Internet Explorer 5 - XML Page Object Type Validation (MS03-
040) |
windows/remote/231[01;31m[K22[m[K.txt

Microsoft Internet Explorer 5.0.1 - Arbitrary File Upload
| windows/remote/306[01;31m[K22[m[K.html

Microsoft Internet Explorer 5/6 - 'file://' Request Zone Bypass
| windows/remote/[01;31m[K22[m[K575.txt

Microsoft Internet Explorer 5/6 - MSXML XML File Parsing Cross-Site
Scripting |
windows/remote/[01;31m[K22[m[K783.txt

Microsoft Internet Explorer 5/6 - Self Executing HTML File
| windows/remote/[01;31m[K22[m[K288.txt

Microsoft Internet Explorer 5/6 / Mozilla 1.2.1 - URI Display
Obfuscation (1) |
windows/remote/234[01;31m[K22[m[K.txt

Microsoft Internet Explorer 6 - '%USERPROFILE%' File Execution
| windows/remote/[01;31m[K22[m[K734.html

Microsoft Internet Explorer 6 - Frame Src Denial of Service
| windows/dos/29[01;31m[K22[m[K9.txt

Microsoft Internet Explorer 9 - Cross-Site Scripting Filter Bypass
| windows/dos/[01;31m[K22[m[K100.txt

Microsoft Internet Explorer 9 - Memory Corruption Crash (PoC)
| windows/dos/[01;31m[K22[m[K401.php

Microsoft Internet Explorer 9 - MSHTML CMarkup::ReloadInCompatView Use-
After-Free | windows/dos/409[01;31m[K22[m[K.html

Microsoft Internet Explorer 9 - MSHTML CPtsTextParaclient::CountApes
Out-of-Bounds Read |
windows/dos/407[01;31m[K22[m[K.html

Microsoft ISA Server 2000 - Cross-Site Scripting
| windows/remote/[01;31m[K22[m[K919.txt

Microsoft Java Virtual Machine 3802 Series - Bytecode Verifier
| windows/remote/[01;31m[K22[m[K027.txt

Microsoft Lync 2010 4.0.7577.0 - User-Agent Header Handling Arbitrary Command Execution |
windows/remote/38[01;31m[K22[m[K7.txt

Microsoft MsMpEng - mpengine x86 Emulator Heap Corruption in VFS API
| windows/dos/4[01;31m[K22[m[K64.txt

Microsoft NetMeeting 2.1/3.0.1 4.4.3385 - CALLTO URL Buffer Overflow (PoC) |
windows/dos/[01;31m[K22[m[K621.txt

Microsoft Office 365 Version 18.2305.1[01;31m[K22[m[K2.0 - Elevation of Privilege + RCE. |
multiple/remote/51609.txt

Microsoft Office OneNote 2010 - Crash (PoC)
| windows/dos/[01;31m[K22[m[K850.txt

Microsoft Office Picture Manager 2010 - Crash (PoC)
| windows/dos/[01;31m[K22[m[K237.txt

Microsoft Office SharePoint Server 2007 - Remote Code Execution (MS10-104) (Metasploit) |
windows/remote/201[01;31m[K22[m[K.rb

Microsoft Office Web Components Spreadsheet - ActiveX 'OWC10/11' Remote Overflow |
windows/remote/9[01;31m[K22[m[K4.py

Microsoft Outlook 5.5/2000 - Web Access HTML Attachment Script Execution |
windows/remote/[01;31m[K22[m[K869.html

Microsoft Outlook Express 5/6 - Script Execution
| windows/remote/[01;31m[K22[m[K959.txt

Microsoft Outlook2000/Express 6.0 - Arbitrary Program Execution
| windows/remote/[01;31m[K22[m[K280.txt

Microsoft Pocket Internet Explorer 3.0 - Denial of Service
| windows/dos/[01;31m[K22[m[K119.html

Microsoft PowerPoint 2003 - '.ppt' File Closure Memory Corruption
| windows/remote/28[01;31m[K22[m[K6.c

Microsoft PowerPoint 2003 - 'mso.dll' '.PPT' Processing Code Execution
| windows/remote/28[01;31m[K22[m[K4.c

Microsoft PowerPoint 2003 - 'powerpnt.exe' Remote Overflow
| windows/remote/28[01;31m[K22[m[K5.c

Microsoft Publisher 2010 - Crash (PoC)
| windows/dos/[01;31m[K22[m[K310.txt

Microsoft Publisher 2013 - Crash (PoC)
| windows/dos/[01;31m[K22[m[K655.txt

Microsoft Silverlight - ScriptObject Unsafe Memory Access (MS13-
0[01;31m[K22[m[K/MS13-087) (Metasploit) |
windows/local/41702.rb

Microsoft SQL Server 7.0/2000 / MSDE - Named Pipe Denial of Service
(MS03-031) |
windows/dos/[01;31m[K22[m[K957.cpp

Microsoft SQL Server 7.0/2000 JET Database Engine 4.0 - Buffer Overrun
| windows/dos/[01;31m[K22[m[K576.txt

Microsoft Visio 2010 - Crash (PoC)
| windows/dos/[01;31m[K22[m[K679.txt

Microsoft Windows - '.png' IHDR Block Denial of Service (PoC) (2)
| windows/dos/[01;31m[K22[m[K10.c

Microsoft Windows - '.png' IHDR Block Denial of Service (PoC) (3)
| windows/dos/[01;31m[K22[m[K04.c

Microsoft Windows - '0x[01;31m[K22[m[K4000 IOCTL (WmiQueryAllData)'
Kernel WMIDataDevice Pool Memory Disclosure |
windows/dos/4[01;31m[K22[m[K13.cpp

Microsoft Windows - 'ATMFD.DLL' CFF table (ATMFD+0x34072 /
ATMFD+0x3407b) Invalid Memory Access |
windows/dos/379[01;31m[K22[m[K.txt

Microsoft Windows - 'IOCTL 0x390400_ operation code 0x00020000' Kernel
KsecDD Pool Memory Disclosure |
windows/dos/4[01;31m[K22[m[K11.cpp

Microsoft Windows - 'IOCTL_DISK_GET_DRIVE_GEOMETRY_EX' Kernel partmgr
Pool Memory Disclosure |
windows/dos/4[01;31m[K22[m[K16.cpp

Microsoft Windows - 'IOCTL_DISK_GET_DRIVE_LAYOUT_EX' Kernel partmgr
Pool Memory Disclosure |
windows/dos/4[01;31m[K22[m[K17.cpp

Microsoft Windows - 'IOCTL_MOUNTMGR_QUERY_POINTS' Kernel Mountmgr Pool
Memory Disclosure |
windows/dos/4[01;31m[K22[m[K12.cpp

Microsoft Windows - 'IOCTL_VOLUME_GET_VOLUME_DISK_EXTENTS' volmgr Pool Memory Disclosure | windows/dos/4[01;31m[K22[m[K15.cpp

Microsoft Windows - 'nt!KiDispatchException' Kernel Stack Memory Disclosure in Exception Handling | windows/dos/4[01;31m[K22[m[K20.cpp

Microsoft Windows - 'nt!NtNotifyChangeDirectoryFile' Kernel Pool Memory Disclosure | windows/dos/4[01;31m[K22[m[K19.cpp

Microsoft Windows - 'nt!NtQueryInformationJobObject (BasicLimitInformation_ ExtendedLimitInformation)' Ker | windows/dos/4[01;31m[K22[m[K28.cpp

Microsoft Windows - 'nt!NtQueryInformationJobObject (information class 12)' Kernel Stack Memory Disclosure | windows/dos/4[01;31m[K22[m[K31.cpp

Microsoft Windows - 'nt!NtQueryInformationJobObject (information class 28)' Kernel Stack Memory Disclosure | windows/dos/4[01;31m[K22[m[K32.cpp

Microsoft Windows - 'nt!NtQueryInformationProcess (ProcessVmCounters)' Kernel Stack Memory Disclosure | windows/dos/4[01;31m[K22[m[K29.cpp

Microsoft Windows - 'nt!NtQueryInformationResourceManager (information class 0)' Kernel Stack Memory Discl | windows/dos/4[01;31m[K22[m[K42.cpp

Microsoft Windows - 'nt!NtQueryInformationTransaction (information class 1)' Kernel Stack Memory Disclosur | windows/dos/4[01;31m[K22[m[K33.cpp

Microsoft Windows - 'nt!NtQueryInformationWorkerFactory (WorkerFactoryBasicInformation)' Kernel Stack Memo | windows/dos/4[01;31m[K22[m[K44.cpp

Microsoft Windows - 'nt!NtQueryVolumeInformationFile (FileFsVolumeInformation)' Kernel Pool Memory Disclos | windows/dos/4[01;31m[K22[m[K18.cpp

Microsoft Windows - 'USP10!CreateIndexTable' Uniscribe Font Processing Out-of-Bounds Memory Read | windows/dos/4[01;31m[K22[m[K37.txt

Microsoft Windows - 'USP10!MergeLigRecords' Uniscribe Font Processing Heap Memory Corruption | windows/dos/4[01;31m[K22[m[K34.txt

Microsoft Windows - 'USP10!NextCharInLiga' Uniscribe Font Processing Out-of-Bounds Memory Read | windows/dos/4[01;31m[K22[m[K38.txt

Microsoft Windows - 'USP10!otlReverseChainingLookup::apply' Uniscribe Font Processing Out-of-Bounds Memory | windows/dos/4[01;31m[K22[m[K41.txt

Microsoft Windows - 'USP10!otlSinglePosLookup::getCoverageTable' Uniscribe Font Processing Out-of-Bounds M | windows/dos/4[01;31m[K22[m[K39.txt

Microsoft Windows - 'USP10!otlValueRecord::adjustPos' Uniscribe Font Processing Out-of-Bounds Memory Read | windows/dos/4[01;31m[K22[m[K40.txt

Microsoft Windows - 'USP10!SubstituteNtoM' Uniscribe Font Processing Out-of-Bounds Memory Read | windows/dos/4[01;31m[K22[m[K36.txt

Microsoft Windows - 'USP10!ttoGetTableData' Uniscribe Font Processing Out-of-Bounds Memory Read | windows/dos/4[01;31m[K22[m[K35.txt

Microsoft Windows - 'win32k!ClientPrinterThunk' Kernel Stack Memory Disclosure | windows/dos/4[01;31m[K22[m[K27.cpp

Microsoft Windows - 'win32k!NtGdiEnumFonts' Kernel Pool Memory Disclosure | windows/dos/4[01;31m[K22[m[K14.txt

Microsoft Windows - 'win32k!NtGdiExtGetObjectW' Kernel Stack Memory Disclosure | windows/dos/4[01;31m[K22[m[K23.cpp

Microsoft Windows - 'win32k!NtGdiGetOutlineTextMetricsInternalW' Kernel Pool Memory Disclosure | windows/dos/4[01;31m[K22[m[K10.cpp

Microsoft Windows - 'win32k!NtGdiGetOutlineTextMetricsInternalW' Kernel Stack Memory Disclosure | windows/dos/4[01;31m[K22[m[K24.cpp

Microsoft Windows - 'win32k!NtGdiGetRealizationInfo' Kernel Stack Memory Disclosure | windows/dos/4[01;31m[K22[m[K26.cpp

Microsoft Windows - 'win32k!NtGdiGetTextMetricsW' Kernel Stack Memory Disclosure | windows/dos/4[01;31m[K22[m[K25.cpp

```
Microsoft Windows - 'win32k!NtGdiMakeFontDir' Kernel Stack Memory
Disclosure                                  |
windows/dos/4[01;31m[K22[m[K30.txt

Microsoft Windows - ASN.1 Remote (MS04-007)
| windows/remote/30[01;31m[K22[m[K.txt

Microsoft Windows - CanonicalizePathName() Remote (MS06-040)
| windows/remote/[01;31m[K22[m[K23.c

Microsoft Windows - DCOM RPC Interface Buffer Overrun
| windows/remote/[01;31m[K22[m[K917.txt

Microsoft Windows - Font Driver Buffer Overflow (MS15-078) (Metasploit)
| windows_x86-64/local/38[01;31m[K22[m[K2.rb

Microsoft Windows - ListBox/ComboBox Control Local (MS03-045)
| windows/local/1[01;31m[K22[m[K.c

Microsoft Windows - Local Procedure Call (LPC) Privilege Escalation
| windows/local/348[01;31m[K22[m[K.c

Microsoft Windows - NetpIsRemote() Remote Overflow (MS06-040) (2)
| windows/remote/[01;31m[K22[m[K65.c

Microsoft Windows - SMB Client-Side Bug (PoC) (MS10-006)
| windows/dos/1[01;31m[K22[m[K58.py

Microsoft Windows - XRM-MS File NTLM Information Disclosure Spoofing
| windows/local/5[01;31m[K22[m[K77.txt

Microsoft Windows 10 - SMBv3 Tree Connect (PoC)
| windows/dos/41[01;31m[K22[m[K2.py

Microsoft Windows 11 - Kernel Privilege Escalation
| windows/local/5[01;31m[K22[m[K75.c

Microsoft Windows 11 23h2 - CLFS.sys Elevation of Privilege
| windows/local/5[01;31m[K22[m[K70.c

Microsoft Windows 11 Pro 23H2 - Ancillary Function Driver for WinSock
Privilege Escalation                |
windows/local/5[01;31m[K22[m[K84.C++

Microsoft Windows 7/2008 R2 - SMB Client Trans2 Stack Overflow (MS10-
020) (PoC)                          |
windows/dos/1[01;31m[K22[m[K73.py

Microsoft Windows CONTACT - HTML Injection / Remote Code Execution
| windows/local/46[01;31m[K22[m[K2.txt

Microsoft Windows Defender - Controlled Folder Bypass Through UNC Path
| windows/dos/43[01;31m[K22[m[K9.cs
```

Microsoft Windows Help Program - 'WinHlp32.exe' Crash (PoC)
| windows/dos/[01;31m[K22[m[K303.pl

Microsoft Windows Kernel - 'ATMFD.DLL' Out-of-Bounds Read due to Malformed Name INDEX in the CFF Table |
windows/dos/4[01;31m[K22[m[K43.txt

Microsoft Windows Media Player 7.1 - Skin File Code Execution
| windows/remote/[01;31m[K22[m[K570.java

Microsoft Windows Media Services 'nskey.dll' 4.1 - ActiveX Control Remote Buffer Overflow |
windows/dos/3[01;31m[K22[m[K94.html

Microsoft Windows Media Services - Remote (MS03-0[01;31m[K22[m[K)
| windows/remote/48.c

Microsoft Windows NT 4.0/2000 - Media Services 'nsiislog.dll' Remote Buffer Overflow |
windows/remote/[01;31m[K22[m[K837.c

Microsoft Windows NT/2000 - 'cmd.exe' CD Buffer Overflow (PoC)
| windows/dos/[01;31m[K22[m[K245.txt

Microsoft Windows RSH daemon 1.7 - Remote Buffer Overflow
| windows/remote/4[01;31m[K22[m[K2.c

Microsoft Windows Server 2000 - 'RegEdit.exe' Registry Key Value Buffer Overflow | windows/local/[01;31m[K22[m[K528.c

Microsoft Windows Server 2000 - 'telnet.exe' NTLM Authentication
| windows/remote/20[01;31m[K22[m[K2.cpp

Microsoft Windows Server 2000 - Active Directory Remote Stack Overflow
| windows/remote/[01;31m[K22[m[K782.py

Microsoft Windows Server 2000 - CreateFile API Named Pipe Privilege Escalation (1) |
windows/local/[01;31m[K22[m[K882.c

Microsoft Windows Server 2000 - CreateFile API Named Pipe Privilege Escalation (2) |
windows/local/[01;31m[K22[m[K883.c

Microsoft Windows Server 2000 - Help Facility '.CNT' File :Link Buffer Overflow |
windows/local/[01;31m[K22[m[K354.c

Microsoft Windows Task Scheduler (XP/2000) - '.job' (MS04-0[01;31m[K22[m[K) |
windows/local/353.c

Microsoft Windows VCF or Contact' File - URL Manipulation-Spoof Arbitrary Code Execution | windows/remote/46[01;31m[K22[m[K0.txt

Microsoft Windows XP - HCP URI Buffer Overflow | windows/dos/[01;31m[K22[m[K232.txt

Microsoft Windows XP - Redirector Privilege Escalation | windows/local/[01;31m[K22[m[K[01;31m[K22[m[K5.txt

Microsoft Windows XP - Task Scheduler '.job' Universal (MS04-0[01;31m[K22[m[K) | windows/local/368.c

Microsoft Windows XP/2000 - 'RunDLL32.exe' Local Buffer Overflow | windows/local/[01;31m[K22[m[K870.txt

Microsoft Windows XP/2000 - Fontview Denial of Service | windows/dos/[01;31m[K22[m[K132.txt

Microsoft Windows XP/2000 - Registry Access Local Denial of Service | windows/dos/28[01;31m[K22[m[K7.txt

Microsoft Windows XP/2000/2003 - Keyboard Event Privilege Escalation | windows/local/26[01;31m[K22[m[K2.c

Microsoft Windows XP/2000/2003 - Message Queuing Service Heap Overflow | windows/remote/23[01;31m[K22[m[K9.cpp

Microsoft Windows XP/2000/NT 4.0 - HTML Converter HR Align Buffer Overflow | windows/remote/[01;31m[K22[m[K824.txt

Microsoft Windows XP/2000/NT 4.0 - Locator Service Buffer Overflow | windows/remote/[01;31m[K22[m[K194.txt

Microsoft Windows XP/2000/NT 4.0 - NetDDE Privilege Escalation (1) | windows/local/219[01;31m[K22[m[K.c

Microsoft Windows XP/95/98/2000/NT 4.0 - 'Riched20.dll' Attribute Buffer Overflow | windows/dos/[01;31m[K22[m[K255.txt

Microsoft Windows XP/ME - Help and Support Center Buffer Overflow | windows/remote/[01;31m[K22[m[K289.c

Microsoft Word - Local Machine Zone Code Execution (MS15-0[01;31m[K22[m[K) | windows/local/37657.txt

Microsoft Word 2007/2010/2013/2016 - Out-of-Bounds Read Code Execution (MS16-099) | windows/local/40[01;31m[K22[m[K4.txt

Microsoft Word 2010 - Crash (PoC)
| windows/dos/[01;31m[K22[m[K215.txt

Microsoft Word Document - Malformed Pointer (PoC)
| windows/dos/29[01;31m[K22[m[K.txt

Microsoft Works 8.0 Spreadsheet - Multiple Vulnerabilities
| windows/dos/28[01;31m[K22[m[K2.txt

Microtik SSH Daemon 6.44.3 - Denial of Service (PoC)
| hardware/dos/48[01;31m[K22[m[K8.txt

MidHosting FTP Daemon 1.0.1 - Shared Memory Local Denial of Service
| linux/dos/[01;31m[K22[m[K796.php

Mihalism Multi Host 4.0.0 - Arbitrary File Upload
| php/webapps/1[01;31m[K22[m[K24.txt

Mike Bobbitt Album.PL 0.61 - Remote Command Execution
| cgi/webapps/[01;31m[K22[m[K545.pl

Mini SQL 1.0/1.3 - Remote Format String
| unix/remote/[01;31m[K22[m[K964.c

MiniBill 1.[01;31m[K22[m[Kb - config[plugin_dir] Remote File Inclusion
| php/webapps/[01;31m[K22[m[K72.txt

MiniHTTPServer Web Forums Server 1.x/2.0 - Directory Traversal
| windows/remote/[01;31m[K22[m[K795.txt

Minio 20[01;31m[K22[m[K-07-29T19-40-48Z - Path traversal
| go/webapps/51734.py

mIRC 6.34 - PRIVMSG Handling Stack Buffer Overflow (Metasploit)
| windows/remote/164[01;31m[K22[m[K.rb

Mitsubishi Electric & INEA SmartRTU - Source Code Disclosure
| hardware/webapps/504[01;31m[K22[m[K.txt

Miyabi CGI Tools 1.02 - 'index.pl' Remote Command Execution
| cgi/webapps/34[01;31m[K22[m[K3.txt

MJM QuickPlayer 1.00 Beta 60a / QuickPlayer 2010 - '.s3m' Local Stack
Buffer Overflow (Metasploit) |
windows/local/17[01;31m[K22[m[K9.rb

MNOGoSearch 3.1.20 - 'search.cgi?UL' Remote Buffer Overflow (1)
| cgi/remote/[01;31m[K22[m[K753.pl

MNOGoSearch 3.1.20 - 'search.cgi?UL' Remote Buffer Overflow (2)
| cgi/remote/[01;31m[K22[m[K754.pl

```
Moa Gallery 1.2.0 - Multiple Remote File Inclusions
| php/webapps/95[01;31m[K22[m[K.txt

MobileCartly 1.0 - Arbitrary File Write
| php/webapps/204[01;31m[K22[m[K.txt

Moby NetSuite 1.0/1.2 - POST Handler Buffer Overflow
| multiple/dos/[01;31m[K22[m[K053.txt

Mocha LPD 1.9 - Remote Buffer Overflow (Denial of Service) (PoC)
| windows/dos/1[01;31m[K22[m[K40.py

MOD Guthabenhack 1.3 For Woltlab Burning Board - SQL Injection
| php/webapps/[01;31m[K22[m[K977.txt

Mod_Gzip 1.3.x - Debug Mode
| unix/remote/[01;31m[K22[m[K699.c

Mod_NTLM 0.x - Authorisation Format String
| multiple/dos/[01;31m[K22[m[K514.txt

Mod_NTLM 0.x - Authorisation Heap Overflow
| multiple/dos/[01;31m[K22[m[K512.txt

MoinMoin - twikidraw Action Traversal Arbitrary File Upload
(Metasploit)                                        |
linux/remote/264[01;31m[K22[m[K.rb

Mole Group Real Estate Script 1.1 - SQL Injection
| php/webapps/60[01;31m[K22[m[K.txt

Mollensoft Software Enceladus Server Suite 2.6.1/3.9 - Directory
Traversal                                    |
windows/remote/[01;31m[K22[m[K078.txt

Mollensoft Software Enceladus Server Suite 3.9 - 'FTP' Buffer Overflow
| windows/dos/[01;31m[K22[m[K081.pl

Monkey HTTP Daemon 0.4/0.5/0.6 - Excessive POST Data Buffer Overflow
| linux/dos/[01;31m[K22[m[K433.pl

MooPlayer 1.3.0 - 'm3u' Buffer Overflow (SEH) (PoC)
| windows/dos/360[01;31m[K22[m[K.py

MoreGroupWare 0.6.8 - WEBMAIL2_INC_DIR Remote File Inclusion
| php/webapps/[01;31m[K22[m[K948.txt

Movable Type Pro 5.13en - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K151.txt

Movie Rating System 1.0 - SQLi to RCE (Unauthenticated)
| php/webapps/506[01;31m[K22[m[K.py
```

MovieLibrary 1.4.401 - '.dmv' Local Denial of Service
| windows/dos/1[01;31m[K22[m[K28.py

moxftp 2.2 - Banner Parsing Buffer Overflow
| linux/remote/[01;31m[K22[m[K278.pl

Mozilla 1.x / opera 6/7 - Timed document.write Method Cross Domain Policy |
multiple/remote/[01;31m[K22[m[K751.txt

Mozilla 1.x / Opera 7.0 - LiveConnect JavaScript Denial of Service
| multiple/dos/[01;31m[K22[m[K441.txt

Mozilla Browsers - 0xAD (HOST:) Remote Heap Buffer Overrun (2)
| windows/remote/1[01;31m[K22[m[K4.html

Mozilla Firefox 1.5.0.6 - FTP Request Remote Denial of Service
| multiple/dos/[01;31m[K22[m[K44.pl

Mozilla Firefox 3.0.10 - 'KEYGEN' Remote Denial of Service
| multiple/dos/88[01;31m[K22[m[K.txt

Mozilla Suite/Firefox/Thunderbird - Nested Anchor Tag Status Bar Spoofing |
linux/remote/25[01;31m[K22[m[K1.txt

Mozilla Thunderbird 17.0.6 - Input Validation Filter Bypass
| multiple/dos/31[01;31m[K22[m[K3.txt

Mp3 Online Id Tag Editor - Remote File Inclusion
| php/webapps/1[01;31m[K22[m[K19.txt

MP3Info 0.8.5a - Buffer Overflow
| linux/dos/31[01;31m[K22[m[K0.py

MPCSoftWeb 1.0 - Database Disclosure
| asp/webapps/[01;31m[K22[m[K513.txt

mpg123 pre0.59s - Invalid MP3 Header Memory Corruption
| linux/remote/[01;31m[K22[m[K147.c

MTink 0.9.x - Printer Status Monitor Environment Variable Buffer Overflow |
linux/local/[01;31m[K22[m[K189.txt

Multi-Mirror - Arbitrary File Upload
| php/webapps/1[01;31m[K22[m[K23.txt

MultiHTML 1.5 - File Disclosure
| cgi/webapps/[01;31m[K22[m[K204.txt

```
Multiple Printer Providers (Spooler Service) - Local Privilege
Escalation                                    |
windows/local/3[01;31m[K22[m[K0.c

Multiple Vendor AgentX++ - Stack Buffer Overflow (PoC)
| windows/dos/1[01;31m[K22[m[K74.py

Multitech RouteFinder 550 - Remote Memory Corruption
| multiple/dos/[01;31m[K22[m[K345.txt

Mumble Murmur 1.2 - Denial of Service
| linux/dos/34[01;31m[K22[m[K8.txt

mUnky 0.01 - 'index.php' Remote Code Execution
| php/webapps/3[01;31m[K22[m[K50.py

Muratsoft Haber Portal 3.6 - 'tr' SQL Injection
| asp/webapps/[01;31m[K22[m[K94.txt

MusicBee 2.0.4663 - '.m3u' Denial of Service
| windows/dos/263[01;31m[K22[m[K.pl

My Little Forum 1.5 - 'SearchString' SQL Injection
| php/webapps/1[01;31m[K22[m[K5.php

MyABraCaDaWeb 1.0 - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K378.txt

MyBace Light - 'login_check.php' Remote File
| php/webapps/[01;31m[K22[m[K85.txt

MyBB 1.0.1/1.0.2 Notepad - 'usercp.php' HTML Injection
| php/webapps/271[01;31m[K22[m[K.txt

MyBB 1.8.x - Multiple Vulnerabilities
| php/webapps/35[01;31m[K22[m[K4.txt

MyBB Follower User Plugin - SQL Injection
| php/webapps/[01;31m[K22[m[K405.txt

MyBB Moderator Log Notes Plugin 1.1 - Cross-Site Request Forgery
| php/webapps/45[01;31m[K22[m[K4.txt

MyBB OUGC Feedback Plugin 1.8.[01;31m[K22[m[K - Cross-Site Scripting
| php/webapps/49635.txt

MyBB Profile Albums Plugin 0.9 - 'albums.php?album' SQL Injection
| php/webapps/[01;31m[K22[m[K003.txt

MyBloggie 2.1.2/2.1.3 - BBCode IMG Tag HTML Injection
| php/webapps/278[01;31m[K22[m[K.txt
```

MyBulletinBoard (MyBB) 1.0 - Multiple SQL Injections
| php/webapps/26[01;31m[K22[m[K8.txt

MyBulletinBoard (MyBB) 1.00 RC4 - 'calendar.php' SQL Injection
| php/webapps/10[01;31m[K22[m[K.pl

MyGuestBK - 'Add.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K22[m[K436.txt

MyGuestBK - Unauthorized Admin Panel Access
| asp/webapps/[01;31m[K22[m[K437.txt

MyNews 4.2.2 - 'themefunc.php' Remote File Inclusion
| php/webapps/3[01;31m[K22[m[K8.txt

MyPBS - 'seasonID' SQL Injection
| php/webapps/75[01;31m[K22[m[K.pl

MyPHP Forum 3.0 (Final) - Multiple SQL Injections
| php/webapps/48[01;31m[K22[m[K.txt

myPHPNuke 1.8.8 - 'Default_Theme' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K133.txt

myPHPNuke 1.8.8 - 'links.php' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K268.txt

myphpPageTool 0.4.3-1 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K208.txt

MyPHPSoft MyPHPLinks 2.1.9/2.2 - SQL Injection Administration Bypassing
| php/webapps/[01;31m[K22[m[K088.txt

MYRE Realty Manager - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K713.txt

Myrephp Business Directory - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K711.txt

MYREphp Vacation Rental Software - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K712.txt

MyRoom 3.5 GOLD - 'save_item.php' Arbitrary File Upload
| php/webapps/[01;31m[K22[m[K186.txt

MyServer 0.4.1 - Remote Denial of Service
| windows/dos/[01;31m[K22[m[K817.pl

myServer 0.4.1 - Signal Handling Denial of Service
| windows/dos/[01;31m[K22[m[K774.txt

MyServer 0.4.1/0.4.2 - HTTP Server Directory Traversal
| windows/remote/[01;31m[K22[m[K785.txt

MyServer 0.4.2 - Malformed URI Denial of Service
| windows/dos/[01;31m[K22[m[K875.txt

MyServer 0.4.3 - GET Argument Buffer Overflow
| linux/dos/[01;31m[K22[m[K700.c

MyServer 0.5 - GET Argument Buffer Overflow
| linux/dos/[01;31m[K22[m[K701.c

MyServer 0.9.8 - Post.MSCGI Cross-Site Scripting
| multiple/remote/30[01;31m[K22[m[K2.txt

Myspace Clone Script - SQL Injection
| php/webapps/46[01;31m[K22[m[K.txt

MySQL 3.20.32/3.[01;31m[K22[m[K.x/3.23.x - Null Root Password Weak
Default Configuration (1) |
linux/remote/21725.c

MySQL 3.20.32/3.[01;31m[K22[m[K.x/3.23.x - Null Root Password Weak
Default Configuration (2) |
linux/remote/21726.c

MySQL 3.[01;31m[K22[m[K.27/3.[01;31m[K22[m[K.29/3.23.8 - GRANT Global
Password Changing |
multiple/local/19721.txt

Mysql 3.[01;31m[K22[m[K.x/3.23.x - Local Buffer Overflow
| linux/local/20581.c

MySQL 3.23.x - 'mysqld' Local Privilege Escalation
| linux/local/[01;31m[K22[m[K340.txt

MySQL 3.23.x/4.0.x - 'COM_CHANGE_USER' Password Length Account
| unix/remote/[01;31m[K22[m[K084.c

MySQL 3.23.x/4.0.x - COM_CHANGE_USER Password Memory Corruption
| unix/remote/[01;31m[K22[m[K085.txt

MySQL 3.x/4.0.x - Weak Password Encryption
| linux/local/[01;31m[K22[m[K565.c

MySQL AB ODBC Driver 3.51 - Plain Text Password
| windows/local/[01;31m[K22[m[K946.txt

N/X Web CMS (N/X WCMS 4.5) - Multiple Vulnerabilities
| php/webapps/1[01;31m[K22[m[K95.txt

N/X Web Content Management System 2002 Prerelease 1 -
'datasets.php?c_path' Local File Inclusion |
php/webapps/[01;31m[K22[m[K116.txt

N/X Web Content Management System 2002 Prerelease 1 - 'menu.inc.php?c_path' Remote File Inclusion | php/webapps/[01;31m[K22[m[K115.txt

Nagios Network Analyzer 2.2.1 - Multiple Cross-Site Request Forgery Vulnerabilities | php/webapps/40[01;31m[K22[m[K1.txt

Nagios XI 5.5.6 - Remote Code Execution / Privilege Escalation | linux/webapps/46[01;31m[K22[m[K1.py

Nagios XI 5.7.X - Remote Code Execution RCE (Authenticated) | php/webapps/494[01;31m[K22[m[K.py

Nagios XI Network Monitor Graph Explorer Component - Command Injection (Metasploit) | unix/remote/23[01;31m[K22[m[K7.rb

NagVis 1.9.33 - Arbitrary File Read | php/webapps/5[01;31m[K22[m[K29.py

Narcissus - Remote Command Execution | php/webapps/[01;31m[K22[m[K709.txt

Narcissus Image Configuration - Passthru (Metasploit) | linux/remote/[01;31m[K22[m[K856.rb

NAT32 2.2 Build [01;31m[K22[m[K284 - Cross-Site Request Forgery | windows/webapps/44034.txt

NAT32 2.2 Build [01;31m[K22[m[K284 - Remote Command Execution | windows/webapps/44033.txt

Nero MediaHome 4.5.8.0 - Denial of Service | windows/dos/240[01;31m[K22[m[K.txt

NES Game and NES System c1081[01;31m[K22[m[K - Remote File Inclusion | php/webapps/[01;31m[K22[m[K26.txt

Nessus 2.0.x - LibNASL Arbitrary Code Execution | multiple/dos/[01;31m[K22[m[K634.txt

NetBackup 7.0 - 'NetBackup INET Daemon' Unquoted Service Path | windows/local/48[01;31m[K22[m[K7.txt

NetBSD - 'Stack Clash' (PoC) | netbsd_x86/dos/4[01;31m[K22[m[K72.c

NetBSD 5.0.1 - 'IRET' General Protection Fault Handling Privilege Escalation | bsd/local/33[01;31m[K22[m[K9.c

NetClassifieds 1.9.7 - Multiple Input Validation Vulnerabilities | php/webapps/30[01;31m[K22[m[K3.txt

NetDrive 2.6.12 - Unquoted Service Path Privilege Escalation
| windows/local/404[01;31m[K22[m[K.txt

Netgear DGN1000 / DGN[01;31m[K22[m[K00 - Multiple Vulnerabilities
| hardware/webapps/25978.txt

Netgear DGN[01;31m[K22[m[K00 - 'dnslookup.cgi' Command Injection
(Metasploit) |
cgi/remote/4[01;31m[K22[m[K57.rb

Netgear DGN[01;31m[K22[m[K00 / DGND3700 - Admin Password Disclosure
| hardware/webapps/46764.sh

Netgear DGN[01;31m[K22[m[K00 1.0.0.29_1.7.29_HotS - Password Disclosure
| hardware/webapps/34149.txt

Netgear DGN[01;31m[K22[m[K00 1.0.0.29_1.7.29_HotS - Persistent Cross-
Site Scripting |
hardware/webapps/33138.txt

Netgear DGN[01;31m[K22[m[K00 N300 Wireless Router - Multiple
Vulnerabilities |
hardware/webapps/31617.txt

Netgear DGN[01;31m[K22[m[K00B - 'pppoe.cgi' Remote Command Execution
(Metasploit) |
hardware/remote/24974.rb

Netgear DGN[01;31m[K22[m[K00B - Multiple Vulnerabilities
| hardware/webapps/24513.txt

Netgear DGN[01;31m[K22[m[K00v1 - Remote Command Execution (RCE)
(Unauthenticated) |
hardware/webapps/50099.py

Netgear DGN[01;31m[K22[m[K00v1/v2/v3/v4 - 'dnslookup.cgi' Remote
Command Execution |
hardware/webapps/41459.py

Netgear DGN[01;31m[K22[m[K00v1/v2/v3/v4 - 'ping.cgi' Remote Command
Execution |
hardware/webapps/41394.py

Netgear DGN[01;31m[K22[m[K00v1/v2/v3/v4 - Cross-Site Request Forgery
| hardware/webapps/41472.html

Netgear FM114P ProSafe Wireless Router - Rule Bypass
| hardware/remote/[01;31m[K22[m[K455.txt

Netgear FM114P ProSafe Wireless Router - UPnP Information Disclosure
| hardware/remote/[01;31m[K22[m[K453.txt

Netgear FM114P Wireless Firewall - File Disclosure
| hardware/remote/[01;31m[K22[m[K236.txt

Netgear ProSafe 1.x - VPN Firewall Web Interface Login Denial of Service |
hardware/dos/[01;31m[K22[m[K407.txt

Nethack 3 - Local Buffer Overflow (1)
| linux/local/[01;31m[K22[m[K233.c

Nethack 3 - Local Buffer Overflow (2)
| linux/local/[01;31m[K22[m[K234.c

Nethack 3 - Local Buffer Overflow (3)
| linux/local/[01;31m[K22[m[K235.pl

NetIQ Privileged User Manager 2.3.1 - 'ldapagnt_eval()' Perl Remote Code Execution (Metasploit) |
windows/remote/[01;31m[K22[m[K903.rb

Netis ADSL Router DL43[01;31m[K22[m[KD RTK 2.1.1 - Cross-Site Request Forgery (Add Admin) |
hardware/webapps/45532.txt

Netis ADSL Router DL43[01;31m[K22[m[KD RTK 2.1.1 - Cross-Site Scripting
| hardware/webapps/454[01;31m[K22[m[K.txt

Netis ADSL Router DL43[01;31m[K22[m[KD RTK 2.1.1 - Denial of Service (PoC) |
hardware/dos/45424.py

Netlink GPON Router 1.0.11 - Remote Code Execution
| hardware/webapps/48[01;31m[K22[m[K5.txt

NetOffice Dwins 1.4p3 - SQL Injection
| php/webapps/[01;31m[K22[m[K590.txt

NetOp Remote Control 8.0/9.1/9.2/9.5 - Local Buffer Overflow
| windows/local/17[01;31m[K22[m[K3.pl

Netscape 6.0/7.0 - Style Sheet Denial of Service
| unix/dos/[01;31m[K22[m[K286.html

Netscape 7.0 - JavaScript Regular Expression Denial of Service
| unix/dos/[01;31m[K22[m[K287.html

Netscape Enterprise Server 3.x/4.x - PageServices Information Disclosure |
multiple/remote/[01;31m[K22[m[K611.txt

Netscape Enterprise Server 4.1 - HTTP Method Name Buffer Overflow
| multiple/dos/[01;31m[K22[m[K230.pl

NetScreen ScreenOS 4.0.1/4.0.3 - TCP Window Size Remote Denial of Service |
windows/dos/[01;31m[K22[m[K970.txt

NetSuite 1.0/1.2 - HTTP Server Directory Traversal
| windows/remote/[01;31m[K22[m[K909.txt

NetWin SurgeFTP - (Authenticated) Admin Command Injection (Metasploit)
| multiple/remote/235[01;31m[K22[m[K.rb

Netwrix Auditor 7.1.3[01;31m[K22[m[K.0 - ActiveX 'sourceFile' Stack Buffer Overflow |
windows/dos/39565.txt

News Evolution 1.0/2.0 - Include Undefined Variable Command Execution
| php/webapps/[01;31m[K22[m[K048.txt

NewsHOWLER 1.03 - Cookie Data SQL Injection
| php/webapps/3[01;31m[K22[m[K71.txt

NewsReactor 20070[01;31m[K22[m[K0 - Article Grabbing Remote Buffer Overflow (1) |
windows/remote/3462.cpp

NewsReactor 20070[01;31m[K22[m[K0 - Article Grabbing Remote Buffer Overflow (2) |
windows/remote/3463.cpp

Newsscript 1.0 - Administrative Privilege Escalation
| php/webapps/[01;31m[K22[m[K663.txt

Nginx 0.7.65/0.8.39 (dev) - Source Disclosure / Download
| windows/remote/138[01;31m[K22[m[K.txt

Nginx 1.4.0 (Generic Linux x64) - Remote Overflow
| linux_x86-64/remote/3[01;31m[K22[m[K77.txt

NOCC Webmail 1.0 - Local File Inclusion / Remote Code Execution
| php/webapps/15[01;31m[K22[m[K.php

Nokia IPSO 3.4.x - Voyager ReadFile.TCL Remote File Reading
| hardware/remote/[01;31m[K22[m[K533.txt

Nokia SGSN DX200 - Remote SNMP Information Disclosure
| hardware/remote/[01;31m[K22[m[K350.txt

Nortel Networks SRG V16 - 'admin_modules.php?module' Traversal Local File Inclusion |
php/webapps/3[01;31m[K22[m[K46.txt

Nortel Networks SRG V16 - 'modules.php?module' Cross-Site Scripting
| php/webapps/3[01;31m[K22[m[K45.txt

Nortel Networks SRG V16 - 'modules.php?module' Traversal Local File Inclusion |
php/webapps/3[01;31m[K22[m[K47.txt

Nortel Wireless LAN Access Point [01;31m[K22[m[K00 Series - Denial of Service |
hardware/dos/23786.c

Novell eDirectory 8.8 SP5 - (Authenticated) Remote Buffer Overflow
| novell/remote/110[01;31m[K22[m[K.pl

Novell File Reporter (NFR) Agent FSFUI Record - Arbitrary File Upload / Remote Code Execution (Metasploit) |
windows/remote/[01;31m[K22[m[K787.rb

Novell Groupwise Client 7.0.3.1294 - 'gxmim1.dll' ActiveX Control Buffer Overflow (PoC) |
windows/dos/33[01;31m[K22[m[K1.html

Novell Groupwise Internet Agent - LDAP BIND Request Overflow
| windows/dos/[01;31m[K22[m[K707.txt

Novell NetIQ Privileged User Manager 2.3.1 - 'auth.dll' pa_modify_accounts() Remote Code Execution |
windows/remote/[01;31m[K22[m[K737.txt

Novell NetIQ Privileged User Manager 2.3.1 - 'ldapagnt.dll' ldapagnt_eval() Perl Code Evaluation Remote Co |
windows/remote/[01;31m[K22[m[K738.txt

Novell Netware 6.0 / eDirectory 8.7 - HTTPSTK.NLM Remote Abend
| novell/dos/[01;31m[K22[m[K749.txt

Novell Netware Enterprise Web Server 5.1/6.0 - 'CGI2Perl.NLM' Buffer Overflow (PoC) |
netware/dos/[01;31m[K22[m[K949.txt

NTFS 3.1 - Master File Table Denial of Service
| windows/dos/4[01;31m[K22[m[K53.html

Nucleus CMS 3.[01;31m[K22[m[K - 'action.php' Cross-Site Scripting
| php/webapps/31074.txt

Nucleus CMS 3.[01;31m[K22[m[K - 'DIR_LIBS' Remote File Inclusion
| php/webapps/1816.php

Nucleus CMS 3.51 (DIR_LIBS) - Multiple Vulnerabilities
| php/webapps/1[01;31m[K22[m[K41.txt

Nukebrowser 2.x - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K206.txt

Nuked-klaN 1.3 - Remote Information Disclosure
| php/webapps/[01;31m[K22[m[K277.txt

Nukeviet 2.0 - '/admin/login.php' Cookie Authentication Bypass
| php/webapps/3[01;31m[K22[m[K43.txt

Null HTTPd 0.5 - Remote Heap Corruption
| linux/remote/[01;31m[K22[m[K046.c

NVR SP2 2.0 'nvUnifiedControl.dll 1.1.45.0' - 'SetText()' Command Execution |
windows/remote/43[01;31m[K22[m[K.html

OCE 3121/31[01;31m[K22[m[K Printer - 'parser.exe' Denial of Service
| hardware/dos/1718.pl

Ocean12 ASP Guestbook Manager 1.0 - Information Disclosure
| asp/webapps/[01;31m[K22[m[K484.txt

ocPortal 7.1.5 - 'code_editor.php' Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/370[01;31m[K22[m[K.txt

Omer Portal 3.[01;31m[K22[m[K0060425 - 'arama_islem.asp' Cross-Site Scripting |
asp/webapps/35576.txt

One-News - Multiple Input Validation Vulnerabilities
| php/webapps/3[01;31m[K22[m[K93.txt

Onecenter Forum 4.0 - IMG Tag Script Injection
| php/webapps/[01;31m[K22[m[K543.txt

OneHTTPD 0.8 - Crash (PoC)
| windows/dos/315[01;31m[K22[m[K.py

OneOrZero Helpdesk 1.4 - 'install.php' Administrative Access
| php/webapps/[01;31m[K22[m[K606.py

OneOrZero Helpdesk 1.4 - 'TUpdate.php' SQL Injection
| php/webapps/[01;31m[K22[m[K605.txt

Online Book Store 1.0 - 'bookisbn' SQL Injection
| php/webapps/479[01;31m[K22[m[K.txt

Online Leave Management System 1.0 - Arbitrary File Upload to Shell (Unauthenticated) |
php/webapps/50[01;31m[K22[m[K8.py

Online Marriage Registration System 1.0 - Persistent Cross-Site Scripting |
php/webapps/485[01;31m[K22[m[K.txt

```
Online Traffic Offense Management System 1.0 - Remote Code Execution
(RCE) (Unauthenticated)                |
php/webapps/50[01;31m[K22[m[K1.py

Oops Proxy Server 1.4.[01;31m[K22[m[K - Remote Buffer Overflow (1)
| unix/remote/20495.c

Oops Proxy Server 1.4.[01;31m[K22[m[K - Remote Buffer Overflow (2)
| linux/remote/20496.c

Oops! 1.4.6 - one russi4n proxy-server Heap Buffer Overflow
| bsd/remote/[01;31m[K22[m[K8.c

Open Azimyt CMS 0.[01;31m[K22[m[K - 'lang' Local File Inclusion
| php/webapps/5831.txt

OpenBB 1.0/1.1 - 'board.php' SQL Injection
| php/webapps/[01;31m[K22[m[K519.txt

OpenBB 1.0/1.1 - 'index.php' SQL Injection
| php/webapps/[01;31m[K22[m[K517.txt

OpenBB 1.0/1.1 - 'member.php' SQL Injection
| php/webapps/[01;31m[K22[m[K520.txt

OpenBSD - 'at Stack Clash' Local Privilege Escalation
| openbsd/local/4[01;31m[K22[m[K71.c

OpenBSD 2.x/3.x - CHPass Temporary File Link File Content Revealing
| openbsd/local/[01;31m[K22[m[K210.txt

OpenBSD 3.x - PF RDR Network Information Leakage
| openbsd/remote/[01;31m[K22[m[K858.txt

OpenCart 3.0.3.6 - Cross Site Request Forgery
| php/webapps/49[01;31m[K22[m[K8.txt

OpenCMS 17.0 - Stored Cross Site Scripting (XSS)
| php/webapps/5[01;31m[K22[m[K09.txt

OpenDreamBox 2.0.0 Plugin WebAdmin - Remote Code Execution
| hardware/webapps/4[01;31m[K22[m[K93.txt

OpenEMR 5.0.1.3 - 'manage_site_files' Remote Code Execution
(Authenticated) (2)                    |
php/webapps/501[01;31m[K22[m[K.rb

openEngine 2.0 100[01;31m[K22[m[K6 - Local File Inclusion / Cross-Site
Scripting                                |
php/webapps/15557.txt

Openfire 3.5.2 - 'login.jsp' Cross-Site Scripting
| jsp/webapps/3[01;31m[K22[m[K49.txt
```

```
Openfire 4.6.0 - 'path' Stored XSS
| jsp/webapps/49[01;31m[K22[m[K9.txt

OpenImpro 1.1 - 'image.php' SQL Injection
| php/webapps/6[01;31m[K22[m[K8.txt

OpenKM 5.1.7 - Cross-Site Request Forgery
| jsp/webapps/37[01;31m[K22[m[K0.txt

OpenLDAP 2.4.[01;31m[K22[m[K - 'modrdn' Multiple Vulnerabilities
| linux/dos/34348.txt

Openreglement 1.04 - Local File Inclusion / Remote File Inclusion
| php/webapps/1[01;31m[K22[m[K96.txt

Openscrutin 1.03 - Local File Inclusion / Remote File Inclusion
| php/webapps/1[01;31m[K22[m[K77.txt

OpenSSH server (sshd) 9.8p1 - Race Condition
| linux/remote/5[01;31m[K22[m[K69.c

OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG
Brute Force SSH                    | linux/remote/56[01;31m[K22[m[K.txt

OpenSSL 0.9.x - CBC Error Information Leakage
| linux/remote/[01;31m[K22[m[K264.txt

Opentel Openmairie tel 1.02 - Local File Inclusion
| php/webapps/1[01;31m[K22[m[K12.txt

OpenTopic 2.3.1 - Private Message HTML Injection
| php/webapps/[01;31m[K22[m[K125.txt

Opera 10.50 - integer Overflow
| windows/dos/116[01;31m[K22[m[K.php

Opera 6.0.x/7.0 - Long File Name Remote Heap Corruption
| windows/dos/[01;31m[K22[m[K550.pl

Opera 6.0/7.0 - 'Filename Download' Buffer Overrun
| windows/remote/[01;31m[K22[m[K341.txt

Opera 6.0/7.0 - 'Username' URI Warning Dialog Buffer Overflow
| windows/dos/[01;31m[K22[m[K239.txt

Opera 6.0/7.0 - opera.PluginContext Native Method Denial of Service
| windows/dos/[01;31m[K22[m[K240.txt

Opera 7 - Denial of Service
| windows/dos/[01;31m[K22[m[K844.html

Opera 7 - Image Rendering HTML Injection
| windows/remote/[01;31m[K22[m[K217.txt
```

Opera 7.0 - Error Message History Disclosure
| windows/remote/[01;31m[K22[m[K219.txt

Opera 7.0 - History Object Information Disclosure
| windows/remote/[01;31m[K22[m[K218.txt

Opera 7.0 - JavaScript Console Attribute Injection
| windows/remote/[01;31m[K22[m[K213.txt

Opera 7.0/7.10 - JavaScript Console Single Quote Attribute Injection
| windows/remote/[01;31m[K22[m[K546.txt

Opera 7.10 - Permanent Denial of Service
| multiple/dos/[01;31m[K22[m[K536.txt

Opera 7.20 - Mail Client Policy Circumvention
| windows/remote/[01;31m[K22[m[K951.html

Opera 7.[01;31m[K22[m[K - File Creation and Execution (WebServer)
| windows/remote/127.pl

Opial 1.0 - Arbitrary File Upload / Cross-Site Scripting / SQL
Injection |
php/webapps/91[01;31m[K22[m[K.txt

Oracle Database - Protocol Authentication Bypass
| multiple/local/[01;31m[K22[m[K069.py

Oracle Database Client System Analyzer - Arbitrary File Upload
(Metasploit) |
windows/remote/[01;31m[K22[m[K714.rb

Oracle Java Runtime Environment - Heap Corruption During TTF font
Rendering in sc_FindExtrema4 |
multiple/dos/467[01;31m[K22[m[K.txt

Oracle MySQL < 5.1.49 - 'DDL' Statements Denial of Service
| linux/dos/345[01;31m[K22[m[K.txt

Oracle Outside In MDB - File Parsing Stack Buffer Overflow (PoC)
| windows/dos/31[01;31m[K22[m[K2.py

Oracle Solaris 11.1/11.3 (RSH) - 'Stack Clash' Local Privilege
Escalation |
solaris_x86/local/4[01;31m[K22[m[K70.c

Oracle VM VirtualBox - 3D Acceleration Multiple Vulnerabilities
| multiple/dos/3[01;31m[K22[m[K08.txt

Oracle VM VirtualBox 4.1 - Local Denial of Service
| linux_x86-64/dos/21[01;31m[K22[m[K4.c

Oracle WebCenter Sites (FatWire Content Server) - Multiple Vulnerabilities |
multiple/webapps/[01;31m[K22[m[K041.txt

OrientDB 2.2.2 < 2.2.[01;31m[K22[m[K - Remote Code Execution (Metasploit) |
multiple/remote/42965.rb

Oscailt CMS 3.3 - Local File Inclusion
| php/webapps/99[01;31m[K22[m[K.txt

osCommerce 2.1/2.2 - 'Checkout_Payment.php' Error Output Cross-Site Scripting |
php/webapps/[01;31m[K22[m[K393.txt

osCommerce 2.1/2.2 - Error_Message Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K391.txt

osCommerce 2.1/2.2 - Info_Message Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K392.txt

osCommerce 2.2 - 'product_info.php' Denial of Service
| php/dos/[01;31m[K22[m[K494.txt

osCommerce 2.2 - Authentication Bypass
| php/webapps/[01;31m[K22[m[K498.txt

osTicket 1.12 - Formula Injection
| php/webapps/47[01;31m[K22[m[K5.txt

osTicket 1.12 - Persistent Cross-Site Scripting
| php/webapps/47[01;31m[K22[m[K6.txt

osTicket 1.12 - Persistent Cross-Site Scripting via File Upload
| php/webapps/47[01;31m[K22[m[K4.txt

osTicket STS 1.2 - Attachment Remote Command Execution
| php/webapps/24[01;31m[K22[m[K5.php

OTRS 3.1 - Persistent Cross-Site Scripting
| windows/webapps/[01;31m[K22[m[K070.py

OTRS 3.x - FAQ Module Persistent Cross-Site Scripting
| multiple/webapps/249[01;31m[K22[m[K.txt

otsAV 1.77.001 - '.ofl' Local Heap Overflow (PoC)
| windows/dos/9[01;31m[K22[m[K8.pl

OTSCMS 2.1.3 - Multiple Remote File Inclusions
| php/webapps/26[01;31m[K22[m[K.txt

Outblaze Webmail - Cookie Authentication Bypass
| cgi/webapps/[01;31m[K22[m[K364.c

```
Ovidentia 6.6.5 - 'index.php' Cross-Site Scripting
| php/webapps/3[01;31m[K22[m[K72.txt

Owl Intranet Engine 0.7 - Authentication Bypass
| php/webapps/[01;31m[K22[m[K600.txt

Owl Intranet Engine 0.95 - 'register.php' Cross-Site Scripting
| php/webapps/321[01;31m[K22[m[K.txt

P-News 1.16 - Administrative Account Creation
| multiple/remote/[01;31m[K22[m[K649.txt

pablo software Solutions baby ftp server 1.2 - Directory Traversal
| windows/remote/[01;31m[K22[m[K691.txt

Pablo Software Solutions FTP Service 1.2 - Anonymous Users Privileges
| windows/remote/[01;31m[K22[m[K721.txt

Pablo Software Solutions FTP Service 1.2 - Plaintext Password
| windows/remote/[01;31m[K22[m[K7[01;31m[K22[m[K.txt

PABox 1.6 - Password Reset
| php/webapps/[01;31m[K22[m[K845.txt

PABox 2.0 - Post Icon HTML Injection
| php/webapps/25[01;31m[K22[m[K0.txt

Painkiller 1.3.1 - Denial of Service
| windows/dos/4[01;31m[K22[m[K.c

PalmOS 3/4 - ICMP Flood Remote Denial of Service
| palm_os/dos/[01;31m[K22[m[K602.c

Panda Global Protection 2010 - Local Denial of Service
| windows/dos/160[01;31m[K22[m[K.c

PaperCut NG/MG [01;31m[K22[m[K.0.4 - Authentication Bypass
| multiple/webapps/51391.py

PaperCut NG/MG [01;31m[K22[m[K.0.4 - Remote Code Execution (RCE)
| multiple/webapps/51452.py

Passlog Daemon 0.1 - 'SL_Parse' Remote Buffer Overflow (1)
| unix/remote/[01;31m[K22[m[K449.c

Passlog Daemon 0.1 - 'SL_Parse' Remote Buffer Overflow (2)
| unix/remote/[01;31m[K22[m[K450.c

Pay Banner Text Link Ad 1.0.6.1 - Cross-Site Request Forgery (Update
Admin)                                    |
php/webapps/426[01;31m[K22[m[K.html
```

PBLang 4.0/4.56 Bulletin Board System - IMG Tag HTML Injection
| php/webapps/[01;31m[K22[m[K960.txt

PDF Complete 3.5.310.2002 - 'pdfsvc.exe' Unquoted Service Path
| windows/local/49[01;31m[K22[m[K6.txt

pdfium - opj_j2k_read_mcc 'libopenjpeg' Heap Out-of-Bounds Read
| multiple/dos/393[01;31m[K22[m[K.txt

PEEL 1.0b - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K114.txt

Peel Shopping 2.8/ 2.9 - Cross-Site Scripting / SQL Injections
| php/webapps/184[01;31m[K22[m[K.txt

Perception LiteServe 2.0 - CGI Source Disclosure
| multiple/remote/[01;31m[K22[m[K020.pl

Perl2Exe 1.0 9/5.0 2/6.0 - Code Obfuscation
| multiple/local/[01;31m[K22[m[K272.pl

Petraware pTransformer ADC < 2.1.7.[01;31m[K22[m[K827 - Login Bypass
| windows/remote/46934.txt

PG Dating Pro CMS 1.0 - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K373.txt

PGP4Pine 1.75.6/1.76 - 'Message Line' Remote Buffer Overflow
| linux/remote/[01;31m[K22[m[K346.c

Phaos 0.9.2 - 'basename()' Remote Command Execution
| php/webapps/[01;31m[K22[m[K53.php

Pheap CMS 1.1 - 'lpref' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K81.pl

Phenotype CMS 3.0 - SQL Injection
| php/webapps/159[01;31m[K22[m[K.txt

philboard 1.14 - 'philboard_admin.asp' Authentication Bypass
| asp/webapps/[01;31m[K22[m[K673.txt

PHlyMail Lite 3.4.4 - 'folderprops.php' Remote File Inclusion (2)
| php/webapps/[01;31m[K22[m[K36.txt

PHlyMail Lite 3.4.4 - 'mod.listmail.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K11.txt

pHNews alpha 1 - 'templates_dir' Remote Code Execution
| php/webapps/[01;31m[K22[m[K98.php

Phorum 3.4 - Email Subject Line Script Injection
| php/webapps/[01;31m[K22[m[K451.txt

```
Phorum 3.4.x - 'Message Form' HTML Injection
| php/webapps/[01;31m[K22[m[K579.txt

Phorum 5.0.14 - Multiple Subject and Attachment HTML Injection
Vulnerabilities                                 |
php/webapps/25[01;31m[K22[m[K3.txt

PhotoPost < 4.85 - Multiple Vulnerabilities
| php/webapps/438[01;31m[K22[m[K.txt

PHP 3.0.16/4.0.2 - Remote Format Overflow
| linux/remote/[01;31m[K22[m[K0.c

PHP 4 - 'PHPInfo()' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K725.txt

PHP 4.3 - 'socket_iovec_alloc()' Integer Overflow
| php/dos/[01;31m[K22[m[K419.php

PHP 4.3.x - Undefined Safe_Mode_Include_Dir Safemode Bypass
| php/local/[01;31m[K22[m[K911.php

PHP 4.3.x/5.0 - 'openlog()' Buffer Overflow
| php/dos/[01;31m[K22[m[K435.php

PHP 4.x - 'socket_recv()' Signed Integer Memory Corruption
| php/dos/[01;31m[K22[m[K425.php

PHP 4.x - 'socket_recvfrom()' Signed Integer Memory Corruption
| php/dos/[01;31m[K22[m[K426.php

PHP 4.x - DLOpen Memory Disclosure (1)
| php/local/230[01;31m[K22[m[K.c

PHP 4.x - Transparent Session ID Cross-Site Scripting
| php/remote/[01;31m[K22[m[K696.txt

PHP 5.2.3 - 'PHP_gd2.dll' imagepsloadfont Local Buffer Overflow (PoC)
| windows/dos/4[01;31m[K22[m[K7.php

PHP 5.3.3 - NumberFormatter::getSymbol Integer Overflow
| multiple/dos/157[01;31m[K22[m[K.txt

PHP 5.3.x - Denial of Service
| php/dos/1[01;31m[K22[m[K59.php

PHP 5.4/5.5/5.6 - SplObjectStorage 'Unserialize()' Use-After-Free
| php/dos/381[01;31m[K22[m[K.txt

PHP Arena paFileDB 1.1.3/2.1.1/3.0/3.1 - Arbitrary File Upload /
Execution                                       |
php/webapps/[01;31m[K22[m[K955.html
```

```
PHP Classifieds Script 051[01;31m[K22[m[K008 - SQL Injection
| php/webapps/5599.txt

PHP ICalender 2.[01;31m[K22[m[K - 'index.php' Cross-Site Scripting
| php/webapps/28131.txt

PHP Links 1.3 - 'smarty.php' Remote File Inclusion
| php/webapps/50[01;31m[K22[m[K.txt

PHP Multi User Randomizer 2006.09.13 - 'Configure_Plugin.TPL.php'
Cross-Site Scripting                     |
php/webapps/300[01;31m[K22[m[K.txt

PHP Proxima 6 - completepack Remote Code Execution
| php/webapps/[01;31m[K22[m[K99.php

PHP RapidKill Pro 5.x - Arbitrary File Upload
| php/webapps/1[01;31m[K22[m[K72.txt

PHP Realty - 'dpage.php' SQL Injection
| php/webapps/3[01;31m[K22[m[K41.txt

PHP Running Management 1.0.2 - 'index.php' Cross-Site Scripting
| php/webapps/310[01;31m[K22[m[K.txt

PHP Server Monitor - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K881.txt

PHP Support Tickets 2.2 - Code Execution
| php/webapps/178[01;31m[K22[m[K.txt

PHP TopSites 2.0/2.2 - 'edit.php' SQL Injection
| php/webapps/[01;31m[K22[m[K177.txt

PHP TopSites 2.0/2.2 - 'help.php' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K176.txt

PHP TopSites 2.0/2.2 - HTML Injection
| php/webapps/[01;31m[K22[m[K175.txt

PHP TopSites FREE 1.0[01;31m[K22[m[Kb - 'config.php' Remote File
Inclusion                                                |
php/webapps/28791.txt

PHP Uploader Downloader 2.0 - Cross-Site Scripting
| php/webapps/107[01;31m[K22[m[K.txt

PHP-Board 1.0 - User Password Disclosure
| php/webapps/[01;31m[K22[m[K252.txt

PHP-decoda - 'Video Tag' Cross-Site Scripting
| php/webapps/188[01;31m[K22[m[K.txt
```

```
PHP-Fusion 4.01 - 'readmore.php' SQL Injection
| php/webapps/3[01;31m[K22[m[K42.txt

PHP-Fusion Mod Mg User Fotoalbum 1.0.1 - SQL Injection
| php/webapps/15[01;31m[K22[m[K7.txt

PHP-Gastebuch 1.60 - Information Disclosure
| php/webapps/[01;31m[K22[m[K953.txt

PHP-Nuke 5.5/6.0 AvantGo Module - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K347.txt

PHP-Nuke 5.5/6.0 News Module - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K348.txt

PHP-Nuke 5.6/6.0 - Search Engine SQL Injection
| php/webapps/[01;31m[K22[m[K266.php

PHP-Nuke 5.6/6.x - 'banners.php' Banner Manager Password Disclosure
| php/webapps/[01;31m[K22[m[K411.txt

PHP-Nuke 5.6/6.x News Module - 'article.php' SQL Injection
| php/webapps/[01;31m[K22[m[K413.txt

PHP-Nuke 5.6/6.x News Module - 'index.php' SQL Injection
| php/webapps/[01;31m[K22[m[K414.php

PHP-Nuke 5.x/6.0 - Avatar HTML Injection
| php/webapps/[01;31m[K22[m[K211.txt

PHP-Nuke 5.x/6.0/6.5 Beta 1 - Multiple Cross-Site Scripting
Vulnerabilities                                  |
php/webapps/[01;31m[K22[m[K037.txt

PHP-Nuke 5.x/6.x Web_Links Module - SQL Injection
| php/webapps/[01;31m[K22[m[K589.txt

PHP-Nuke 6.0 - 'modules.php' Denial of Service
| php/dos/[01;31m[K22[m[K110.txt

PHP-Nuke 6.0 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K22[m[K103.txt

PHP-Nuke 6.0 - Multiple Full Path Disclosure Vulnerabilities
| php/webapps/[01;31m[K22[m[K102.txt

PHP-Nuke 6.0 - Web Mail Remote PHP Script Execution
| php/webapps/[01;31m[K22[m[K089.txt

PHP-Nuke 6.0 - Web Mail Script Injection
| php/webapps/[01;31m[K22[m[K090.txt
```

```
PHP-Nuke 6.0/6.5 Forum Module - 'viewforum.php' SQL Injection
| php/webapps/[01;31m[K22[m[K424.txt

PHP-Nuke 6.0/6.5 Forum Module - 'viewtopic.php' SQL Injection
| php/webapps/[01;31m[K22[m[K423.txt

PHP-Nuke 6.0/6.5 Web_Links Module - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K598.txt

PHP-Nuke 6.5 (Multiple Downloads Module) - SQL Injection
| php/webapps/[01;31m[K22[m[K597.txt

PHP-Nuke 6.5 - 'modules.php?Username' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K595.txt

PHP-Nuke 6.5 Addon - 'Viewpage.php' File Disclosure
| php/webapps/[01;31m[K22[m[K4[01;31m[K22[m[K.txt

PHP-Nuke Johannes Hass 'Gaestebuch 2.2 Module - 'id' SQL Injection
| php/webapps/313[01;31m[K22[m[K.txt

PHP-Nuke Splatt Forum 3.2 Module - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K349.txt

PHP-Nuke Splatt Forum 4.0 Module - Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K557.txt

PHP-Nuke Splatt Forum 4.0 Module - HTML Injection
| php/webapps/[01;31m[K22[m[K558.txt

PHP-Proxima - 'autohtml.php' Information Disclosure
| php/webapps/[01;31m[K22[m[K603.txt

PHP-Ring Webring System 0.9.1 - Insecure Cookie Handling
| php/webapps/6[01;31m[K22[m[K5.txt

PHP-Ultimate WebBoard 2.0 - 'admindel.php' Multiple Input Validation
Vulnerabilities                       |
php/webapps/3[01;31m[K22[m[K95.txt

PHP-Wiki 1.2/1.3 - Cross-Site Scripting
| php/webapps/216[01;31m[K22[m[K.txt

PHPAccounts 0.5 - 'index.php' Local File Inclusion
| php/webapps/30[01;31m[K22[m[K0.txt

PHPAccounts 0.5 - 'index.php' Multiple SQL Injections
| php/webapps/30[01;31m[K22[m[K1.txt

PHPAdsNew 2.0.4 - 'AdFrame.php' Cross-Site Scripting
| php/webapps/25[01;31m[K22[m[K5.txt
```

phpAtm 1.21 - 'include_location' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K79.txt

PHPay 2.2 - Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K478.txt

PHPay 2.2 - Multiple Full Path Disclosure Vulnerabilities
| php/webapps/[01;31m[K22[m[K477.txt

phpBB 2.0.3 - 'privmsg.php' SQL Injection
| php/webapps/[01;31m[K22[m[K182.pl

phpBB 2.0.3 - 'search.php' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K065.html

phpBB 2.0.3 - Script Injection
| php/webapps/[01;31m[K22[m[K043.txt

phpBB Advanced Quick Reply Hack 1.0/1.1 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K017.txt

phpBB All Topics Mod 1.5.0 - 'start' SQL Injection
| php/webapps/[01;31m[K22[m[K48.pl

phpBB Journals System Mod 1.0.2 RC2 - Remote File Inclusion
| php/webapps/25[01;31m[K22[m[K.py

PHPBB2 - 'Page_Header.php' SQL Injection
| php/webapps/[01;31m[K22[m[K267.php

phpCodeGenie 3.0.2 - 'BEAUT_PATH' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K12.txt

PHPCOIN 1.2.3 - 'session_set.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K54.txt

phpComasy 0.9.1 - 'entry_id' SQL Injection
| php/webapps/8[01;31m[K22[m[K0.txt

phpCommunityCalendar 4.0 - Multiple SQL Injections
| php/webapps/26[01;31m[K22[m[K9.txt

phpDirectorySource 1.0 - Cross-Site Scripting / SQL Injection
| php/webapps/9[01;31m[K22[m[K6.txt

PHPECard 2.1.4 - 'functions.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K75.txt

PHPFootball 1.6 - Remote Database Disclosure
| php/webapps/3[01;31m[K22[m[K6.txt

PHPForum 2.0 RC1 - 'Mainfile.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K887.txt

```
PHPFreeForum 1.0 rc2 - '/part/menu.php' Multiple Cross-Site Scripting
Vulnerabilities                        |
php/webapps/318[01;31m[K22[m[K.txt

PHPGedView 2.5/2.6 - 'Gdbi_interface.php' Cross-Site Scripting
| php/webapps/248[01;31m[K22[m[K.txt

phpGraphy 0.9.13b - Multiple Vulnerabilities
| php/webapps/17[01;31m[K22[m[K6.txt

phpGroupWare 0.9.16.010 - 'GLOBALS[]' Remote Code Execution
| php/webapps/[01;31m[K22[m[K70.php

PHPizabi 0.848b C1 HP3 - 'id' Local File Inclusion
| php/webapps/3[01;31m[K22[m[K51.txt

PHPKB Multi-Language 9 - 'image-upload.php' Authenticated Remote Code
Execution                              |
php/webapps/48[01;31m[K22[m[K1.py

PHPKB Multi-Language 9 - Authenticated Directory Traversal
| php/webapps/48[01;31m[K22[m[K0.py

phpLDAPadmin 0.9.8 - 'template_engine.php' Cross-Site Scripting
| php/webapps/277[01;31m[K22[m[K.txt

PHPLib Team PHPLIB 7.2 - Remote Script Execution
| php/webapps/210[01;31m[K22[m[K.txt

PHPLinks 2.1.2 - Add Site HTML Injection
| php/webapps/[01;31m[K22[m[K180.txt

phpLiteAdmin - 'table' SQL Injection
| php/webapps/38[01;31m[K22[m[K8.txt

phpLiterAdmin 1.0 RC1 - Authentication Bypass
| php/webapps/153[01;31m[K22[m[K.txt

PHPMailer < 5.2.20 with Exim MTA - Remote Code Execution
| php/webapps/4[01;31m[K22[m[K21.py

PhpMesFilms 1.8 - SQL Injection
| php/webapps/1[01;31m[K22[m[K[01;31m[K22[m[K.txt

phpMyAdmin 2.x - Information Disclosure
| php/webapps/[01;31m[K22[m[K798.txt

phpMyFAQ 1.5.1 - 'User-Agent' Remote Shell Injection
| php/webapps/1[01;31m[K22[m[K6.php

phpMyFAQ 3.1.7 - Reflected Cross-Site Scripting (XSS)
| php/webapps/5[01;31m[K22[m[K26.txt
```

phpMyFAQ 3.2.10 - Unintended File Download Triggered by Embedded Frames
| php/webapps/5[01;31m[K22[m[K35.txt

PHPMyShop 1.0 - 'compte.php' SQL Injection
| php/webapps/[01;31m[K22[m[K209.txt

PHPOF 20040[01;31m[K22[m[K6 - 'DB_adodb.class.php' Remote File
Inclusion |
php/webapps/4363.txt

PHPOpenChat 2.3.4/3.0.1 - 'ENGLISH_poc.php' Remote File Inclusion
| php/webapps/25[01;31m[K22[m[K9.txt

PHPOpenChat 2.3.4/3.0.1 - 'poc.php' Remote File Inclusion
| php/webapps/25[01;31m[K22[m[K8.txt

PHPOpenChat 2.3.4/3.0.1 - 'poc_loginform.php?phpbb_root_path' Remote
File Inclusion |
php/webapps/25[01;31m[K22[m[K7.txt

PHPOutsourcing Zorum 3.x - Remote File Inclusion Command Execution
| php/webapps/[01;31m[K22[m[K195.txt

PHPPass 2 - 'AccessControl.php' SQL Injection
| php/webapps/[01;31m[K22[m[K148.txt

PHPPing 0.1 - Remote Command Execution
| php/webapps/[01;31m[K22[m[K336.txt

PHProjekt 6.1 - 'path_pre' Multiple Remote File Inclusions
| php/webapps/[01;31m[K22[m[K35.txt

PHProjekt PhpSimplyGest v1.3. - Stored Cross-Site Scripting (XSS)
| php/webapps/509[01;31m[K22[m[K.txt

PHPRunner 4.2 - 'SearchOption' Blind SQL Injection
| php/webapps/8[01;31m[K22[m[K6.txt

PhpSocial 2.0.0304_20[01;31m[K22[m[K[01;31m[K22[m[K26 - Cross-Site
Request Forgery |
php/webapps/39086.txt

PHPSysInfo 2.0/2.1 - 'index.php' File Disclosure
| php/webapps/[01;31m[K22[m[K457.txt

PHPSysInfo 2.0/2.1 - 'index.php' LNG File Disclosure
| php/webapps/[01;31m[K22[m[K459.txt

PHPVID 1.1 - Cross-Site Scripting / SQL Injection
| php/webapps/64[01;31m[K22[m[K.txt

PHPWCMS 1.4.5 - 'PHPwcms.php' Cross-Site Scripting
| php/webapps/343[01;31m[K22[m[K.txt

Pi3Web 2.0.1 - Denial of Service (PoC)
| windows/dos/[01;31m[K22[m[K.c

Pi3Web 2.0.1 - GET Denial of Service
| windows/dos/[01;31m[K22[m[K587.c

Pi3Web 2.0.2 - SortName Buffer Overflow
| windows/dos/[01;31m[K22[m[K718.c

Pico MP3 Player 1.0 - '.mp3' / '.pls' Local Crash (PoC)
| windows/dos/11[01;31m[K22[m[K8.pl

PicturesPro Photo Cart 3.9 - Search Cross-Site Scripting
| php/webapps/3[01;31m[K22[m[K91.txt

Pie Web M{a_e}sher 0.5.3 - Multiple Remote File Inclusions
| php/webapps/7[01;31m[K22[m[K1.txt

Pie Web m{a_e}sher mod rss 0.1 - Remote File Inclusion
| php/webapps/7[01;31m[K22[m[K5.txt

Pirelli Discus DRG A[01;31m[K22[m[K5 wifi router - WPA2PSK Default
Algorithm |
hardware/remote/8359.py

Piwigo 2.6.0 - 'picture.php?rate' SQL Injection
| php/webapps/35[01;31m[K22[m[K1.txt

Plane 0.23.1 - Server side request forgery (SSRF)
| multiple/webapps/5[01;31m[K22[m[K11.txt

Planetmoon - Guestbook Clear Text Password Retrieval
| cgi/webapps/[01;31m[K22[m[K408.txt

Plastic SCM 10.0.16.56[01;31m[K22[m[K - WebAdmin Server Access
| multiple/webapps/50426.txt

Platform Load Sharing Facility 4/5 - 'LSF_ENVDIR' Local Command
Execution |
multiple/local/[01;31m[K22[m[K628.sh

PlatinumFTPServer 1.0.6 - Arbitrary File Deletion
| windows/remote/[01;31m[K22[m[K113.txt

PlatinumFTPServer 1.0.6 - Directory Traversal
| windows/remote/[01;31m[K22[m[K136.txt

PlatinumFTPServer 1.0.6 - Information Disclosure
| windows/remote/[01;31m[K22[m[K112.txt

Pligg CMS 9.9.5 - Cross-Site Request Forgery / Protection Bypass /
Captcha Bypass |
php/webapps/79[01;31m[K22[m[K.txt

```
pMachine 1.0/2.x - '/lib/' Multiple Script Direct Request Full Path
Disclosures                                |
php/webapps/[01;31m[K22[m[K808.txt

pMachine 1.0/2.x - Multiple Script 'sfx' Full Path Disclosures
| php/webapps/[01;31m[K22[m[K809.txt

pMachine 1.0/2.x - Search Module Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K810.txt

PMachine 2.2.1 - '/Lib.Inc.php' Remote File Inclusion / Command
Execution                                  |
php/webapps/[01;31m[K22[m[K776.txt

PmWiki 2.1.19 - 'Zend_Hash_Del_Key_Or_Index' Remote Command Execution
| php/webapps/[01;31m[K22[m[K91.php

pointcomma 3.8b2 - Remote File Inclusion
| php/webapps/10[01;31m[K22[m[K0.txt

Polymorph 0.4 - Filename Buffer Overflow
| linux/local/[01;31m[K22[m[K633.c

PopojiCMS 2.0.1 - Remote Command Execution (RCE)
| php/webapps/520[01;31m[K22[m[K.py

PoPToP PPTP 1.0/1.1.x - Negative 'read()' Argument Remote Buffer
Overflow                                   |
linux/remote/[01;31m[K22[m[K479.c

PortailPHP mod_phpalbum 2.1.5 - 'chemin' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K71.txt

Portrait Software Portrait Campaign Manager 4.6.1.[01;31m[K22[m[K -
Multiple Cross-Site Scripting Vulnerabilities       |
asp/webapps/33647.txt

Posnic Stock Management System - SQL Injection
| php/remote/44[01;31m[K22[m[K8.php

Postfix 1.1.x - Denial of Service (1)
| linux/dos/[01;31m[K22[m[K981.c

Postfix 1.1.x - Denial of Service (2)
| linux/dos/[01;31m[K22[m[K982.pl

PostNuke 0.6/0.7 Downloads Module - TTitle Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K997.txt

PostNuke 0.6/0.7 web_links Module - TTitle Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K998.txt
```

PostNuke 0.723 - 'user.php' UNAME Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K767.txt

PostNuke 0.723 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K22[m[K761.txt

PostNuke 0.72x Members_List Module - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K439.txt

PostNuke 0.72x Phoenix Glossary Module - SQL Injection
| php/webapps/[01;31m[K22[m[K651.txt

PostNuke 0.72x Stats Module - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K438.txt

PostNuke Phoenix 0.72x - Rating System Denial of Service
| php/dos/[01;31m[K22[m[K660.txt

POWERGAP 2003 - 's0x.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K01.txt

PowerZip 7.06.38950 - 'Filename Handling' Local Buffer Overflow
| windows/local/[01;31m[K22[m[K86.cpp

PRADO PHP Framework 3.2.0 - Arbitrary File Read
| php/webapps/[01;31m[K22[m[K937.txt

Pre Job Board 1.0 - Authentication Bypass
| php/webapps/105[01;31m[K22[m[K.txt

PrestaShop 1.5.1 - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K430.txt

Prime95 29.4b7 - Denial Of Service (PoC)
| windows_x86/dos/45[01;31m[K22[m[K6.py

Prishtina FTP Client 1.x - Remote Denial of Service
| windows/dos/[01;31m[K22[m[K637.pl

Privacyware Privatefirewall 7.0 - Unquoted Service Path Privilege
Escalation |
windows/local/353[01;31m[K22[m[K.txt

Procentia IntelliPen 1.1.12.1520 - 'data.aspx' Blind SQL Injection
| asp/webapps/3[01;31m[K22[m[K12.txt

ProcessMaker 3.5.4 - Local File inclusion
| multiple/webapps/50[01;31m[K22[m[K9.txt

ProConf 6.0 - Insecure Direct Object Reference (IDOR)
| multiple/webapps/5[01;31m[K22[m[K36.txt

```
ProductCart 1.5/1.6/2.0 - 'Custva.asp' SQL Injection
| asp/webapps/[01;31m[K22[m[K864.txt

ProductCart 1.5/1.6/2.0 - 'login.asp' SQL Injection
| asp/webapps/[01;31m[K22[m[K865.txt

ProductCart 1.5/1.6/2.0 - 'MSG.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K22[m[K866.txt

ProductCart 1.5/1.6/2.0 - File Disclosure
| asp/webapps/[01;31m[K22[m[K868.txt

ProFTPd 1.2.x - 'STAT' Denial of Service
| linux/dos/[01;31m[K22[m[K079.sh

Progress Database 9.1 - Environment Variable Privilege Escalation
| linux/local/[01;31m[K22[m[K773.c

Project64 2.3.2 - Denial Of Service (PoC)
| windows_x86/dos/45[01;31m[K22[m[K9.txt

ProjectPier 0.8 - Multiple HTML Injection / Cross-Site Scripting
Vulnerabilities                          |
php/webapps/31[01;31m[K22[m[K9.txt

ProManager 0.73 - 'note.php' SQL Injection
| php/webapps/[01;31m[K22[m[K59.txt

PromoProducts - 'view_product.php' Multiple SQL Injections
| php/webapps/3[01;31m[K22[m[K57.txt

Property Listing Script - 'propid' Blind SQL Injection
| php/webapps/41[01;31m[K22[m[K5.txt

ProQuiz 2.0.0b - Arbitrary File Upload
| php/webapps/16[01;31m[K22[m[K0.py

Prototype of an PHP Application 0.1 - '/ident/loginmodif.php?path_inc'
Remote File Inclusion               |
php/webapps/301[01;31m[K22[m[K.txt

ProtWare HTML Guardian 6.x - Encryption
| multiple/remote/[01;31m[K22[m[K410.pl

Proxifier for Mac 2.19 - Local Privilege Escalation
| macos/local/43[01;31m[K22[m[K5.sh

Proxomitron Proxy Server - GET Remote Denial of Service
| windows/dos/[01;31m[K22[m[K794.txt

Pserv 2.0 - HTTP Request Parsing Buffer Overflow
| linux/dos/[01;31m[K22[m[K059.pl
```

```
Pserv 2.0 - HTTP Version Specifier Buffer Overflow
| linux/dos/[01;31m[K22[m[K056.txt

Pserv 2.0 - User-Agent HTTP Header Buffer Overflow (1)
| linux/remote/[01;31m[K22[m[K057.pl

Pserv 2.0 - User-Agent HTTP Header Buffer Overflow (2)
| linux/remote/[01;31m[K22[m[K058.c

psipuss 1.0 - Multiple SQL Injections
| php/webapps/6[01;31m[K22[m[K6.txt

pSlash 0.7 - 'lvc_include_dir' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K49.txt

Psunami Bulletin Board 0.x - 'Psunami.cgi' Remote Command Execution (1)
| cgi/webapps/[01;31m[K22[m[K169.pl

Psunami Bulletin Board 0.x - 'Psunami.cgi' Remote Command Execution (2)
| cgi/webapps/[01;31m[K22[m[K170.pl

PunkBuster < 1.[01;31m[K22[m[K9 - WebTool Service Remote Buffer
Overflow (Denial of Service) (PoC)                        |
multiple/dos/1819.txt

PXE Server 2.0 - Remote Buffer Overrun
| linux/remote/[01;31m[K22[m[K379.c

Py-Membres 4.0 - SQL Injection
| php/webapps/[01;31m[K22[m[K474.txt

Pymatgen 2024.1 - Remote Code Execution (RCE)
| python/remote/5[01;31m[K22[m[K05.py

Python 2.2/2.3 - Documentation Server Error Page Cross-Site Scripting
| multiple/remote/[01;31m[K22[m[K496.txt

Python < 2.5.2 Imageop Module - 'imageop.crop()' Buffer Overflow
| multiple/dos/10[01;31m[K22[m[K9.txt

QNX RTOS 2.4 - File Disclosure
| linux/local/[01;31m[K22[m[K212.txt

QNX RTOS 6.2 - Application Packager Non-Explicit Path Execution
| linux/local/[01;31m[K22[m[K002.txt

Qpopper 3/4 - 'Username' Information Disclosure
| linux/remote/[01;31m[K22[m[K361.cpp

Qpopper 4.0.8 (Linux) - 'poppassd' Local Privilege Escalation
| linux/local/1[01;31m[K22[m[K9.sh
```

```
Qpopper 4.0.x - Remote Memory Corruption
| linux/remote/[01;31m[K22[m[K342.c

Qt 4.6.3 - Remote Denial of Service
| windows/dos/34[01;31m[K22[m[K7.txt

QuadComm Q-Shop 2.5 - Failure To Validate Credentials
| asp/webapps/[01;31m[K22[m[K885.asp

Qualcomm Eudora 5.0/5.1/6.0 - Long Attachment Filename Denial of
Service (1)                                  |
windows/dos/[01;31m[K22[m[K333.pl

Qualcomm Eudora 5.0/5.1/6.0 - Long Attachment Filename Denial of
Service (2)                                  |
windows/dos/[01;31m[K22[m[K334.pl

Qualcomm Eudora 5.2.1/6.0 - File Attachment Spoofing Variant
| windows/remote/[01;31m[K22[m[K627.pl

Quick Search 1.1.0.189 - search textbox Buffer Overflow (SEH Unicode)
(Egghunter)                            |
windows/local/368[01;31m[K22[m[K.pl

Quick.Cart 3.4 / Quick.CMS 2.4 - Cross-Site Request Forgery
| php/webapps/10[01;31m[K22[m[K4.txt

QuickDate 1.3.2 - SQL Injection
| php/webapps/480[01;31m[K22[m[K.txt

QuickFront 1.0 - File Disclosure
| windows/remote/[01;31m[K22[m[K476.txt

Quicksilver Forums 1.4.1 - SQL Injection
| php/webapps/6[01;31m[K22[m[K3.php

QuickTicket 1.5 - 'qti_usr.php' SQL Injection
| php/webapps/5[01;31m[K22[m[K2.txt

R 3.4.4 (Windows 10 x64) - Buffer Overflow SEH (DEP/ASLR Bypass)
| windows_x86-64/local/471[01;31m[K22[m[K.py

Raidsonic IB-NAS5[01;31m[K22[m[K0 and IB-NAS4[01;31m[K22[m[K0-B -
Multiple Vulnerabilities                                          |
hardware/webapps/24499.txt

RARLAB FAR 1.65/1.70 - File Manager Buffer Overflow
| linux/dos/[01;31m[K22[m[K243.txt

RaspAP 2.6.6 - Remote Code Execution (RCE) (Authenticated)
| php/webapps/50[01;31m[K22[m[K4.py
```

```
Rational ClearCase 4.1 - Portscan Denial of Service
| unix/dos/[01;31m[K22[m[K031.txt

Rconfig 3.x - Chained Remote Code Execution (Metasploit)
| linux/remote/48[01;31m[K22[m[K3.rb

RDPGuard 9.9.9 - Privilege Escalation
| multiple/local/5[01;31m[K22[m[K89.txt

Really Simple Security 9.1.1.1 - Authentication Bypass
| php/webapps/5[01;31m[K22[m[K07.py

RealPlayer 10.5 (6.0.12.1040-1348) - SWF Buffer Overflow (PoC)
| multiple/dos/16[01;31m[K22[m[K.pl

RealPlayer 15.0.6.14(.3g2) - 'WriteAV' Crash (PoC)
| windows/dos/[01;31m[K22[m[K402.txt

RealPlayer 15.0.6.14.3gp - Crash (PoC)
| windows/dos/[01;31m[K22[m[K154.pl

Rebellion Aliens vs Predator 2.[01;31m[K22[m[K - Multiple Memory
Corruption Vulnerabilities                                  |
windows/remote/33971.c

ReciPHP 1.1 - SQL Injection
| php/webapps/[01;31m[K22[m[K742.txt

Red Mombin 0.7 - 'process_login.php' Cross-Site Scripting
| php/webapps/287[01;31m[K22[m[K.txt

Redaxo 4.2.1 - Remote File Inclusion
| php/webapps/1[01;31m[K22[m[K76.txt

RedHat 6.1 / IRIX 6.5.18 - 'lpd' Command Execution
| unix/remote/197[01;31m[K22[m[K.txt

RedHat 9.0 / Slackware 8.1 - '/bin/mail' Carbon Copy Field Buffer
Overrun                                     |
linux/local/[01;31m[K22[m[K695.pl

Rediff Bol 2.0.2 - URL Handling Denial of Service
| windows/dos/[01;31m[K22[m[K196.txt

Rediff Bol 7.0 Instant Messenger - ActiveX Control Information
Disclosure                                      |
windows/remote/26[01;31m[K22[m[K1.txt

Redragon Gaming Mouse - 'REDRAGON_MOUSE.sys' Denial of Service (PoC)
| windows/dos/503[01;31m[K22[m[K.py

Remote Keyboard Desktop 1.0.1 - Remote Code Execution (RCE)
| windows/remote/5[01;31m[K22[m[K99.py
```

```
Restorator 1793 - Denial of Service (PoC)
| windows_x86-64/dos/45[01;31m[K22[m[K3.py

RhinoSoft Serv-U FTPd Server 4.x - 'site chmod' Remote Buffer Overflow
| windows/remote/8[01;31m[K22[m[K.c

Ricon Industrial Cellular Router S99[01;31m[K22[m[KXL - Remote Command
Execution (RCE)                                  |
hardware/webapps/50096.py

Rising Online Virus Scanner [01;31m[K22[m[K.0.0.5 - ActiveX Control
Stack Overflow (Denial of Service)               |
windows/dos/11492.html

River Past Audio Converter 7.7.16 - Denial of Service (PoC)
| windows/dos/463[01;31m[K22[m[K.py

RJ-iTop Network Vulnerability Scanner System - Multiple SQL Injections
| jsp/webapps/1[01;31m[K22[m[K42.txt

Rlpr 2.0 - 'msg()' Multiple Vulnerabilities
| linux/remote/24[01;31m[K22[m[K3.py

RMSOFT Downloads Plus - '/(rmdp) 1.5/1.7 Module for XOOPS down.php?id'
Cross-Site Scripting             |
php/webapps/3[01;31m[K22[m[K16.txt

RMSOFT Downloads Plus - '/(rmdp) 1.5/1.7 Module for XOOPS
search.php?key' Cross-Site Scripting             |
php/webapps/3[01;31m[K22[m[K15.txt

Rockliffe MailSite 5.3.4/6.1.[01;31m[K22[m[K/7.0.3 - HTTP Mail
Management Cross-Site Scripting                  |
cgi/webapps/27115.txt

RosarioSIS 10.8.4 - CSV Injection
| php/webapps/516[01;31m[K22[m[K.txt

Rosoft Media Player 4.1.8 - '.m3u' File Remote Buffer Overflow (PoC)
| windows/dos/51[01;31m[K22[m[K.pl

Roxy WI v6.1.0.0 - Improper Authentication Control
| python/webapps/51[01;31m[K22[m[K6.txt

Roxy WI v6.1.0.0 - Unauthenticated Remote Code Execution (RCE)
| python/webapps/51[01;31m[K22[m[K7.txt

Roxy WI v6.1.1.0 - Unauthenticated Remote Code Execution (RCE) via
ssl_cert Upload                          |
python/webapps/51[01;31m[K22[m[K8.txt
```

RPM Select/Elite 5.0 - '.xml Configuration parsing' Unicode Buffer Overflow (PoC) | windows/dos/1[01;31m[K22[m[K43.py

RSA Authentication Manager 8.2.1.4.0-build13949[01;31m[K22[m[K / < 8.3 P1 - XML External Entity Injection / Cross-Site | java/webapps/44634.txt

RSA ClearTrust 4.6/4.7 - Login Page Cross-Site Scripting | asp/webapps/[01;31m[K22[m[K357.txt

RTTucson Quotations Database - Multiple Vulnerabilities | php/webapps/245[01;31m[K22[m[K.txt

Ruby 1.9 - 'WEBrick::HTTP::DefaultFileHandler' Crafted HTTP Request Denial of Service | multiple/dos/3[01;31m[K22[m[K[01;31m[K22[m[K.rb

Ruby 1.9 - REXML Remote Denial of Service | linux/dos/3[01;31m[K22[m[K92.rb

Ruby 1.9 - Safe Level Multiple Function Restriction Bypass | multiple/remote/3[01;31m[K22[m[K24.rb

Ruby 1.9 dl - Module DL.dlopen Arbitrary Library Access | multiple/remote/3[01;31m[K22[m[K23.rb

Ruckus IoT Controller 1.7.1.0 - Undocumented Backdoor Account | hardware/local/5[01;31m[K22[m[K42.txt

Rukovoditel 3.3.1 - Remote Code Execution (RCE) | php/webapps/513[01;31m[K22[m[K.txt

Rumble 0.25.[01;31m[K22[m[K32 - Denial of Service | windows/dos/17070.py

Rumpus FTP Server 1.3.x/2.0.3 - Stack Overflow Denial of Service | osx/dos/209[01;31m[K22[m[K.txt

RunCMS 1.2/1.3 - 'PMLite.php' SQL Injection | php/webapps/27[01;31m[K22[m[K6.txt

RunCMS 1.6.1 - 'admin.php' Cross-Site Scripting | php/webapps/31[01;31m[K22[m[K5.html

S8Forum 3.0 - Remote Command Execution | php/webapps/[01;31m[K22[m[K134.txt

Sage 1.0 Beta 3 - Content Management System Cross-Site Scripting | windows/remote/[01;31m[K22[m[K270.txt

Sage 1.0 Beta 3 - Content Management System Full Path Disclosure | windows/remote/[01;31m[K22[m[K269.txt

Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)
| unix/remote/[01;31m[K22[m[K468.c

Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)
| unix/remote/[01;31m[K22[m[K469.c

Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)
| unix/remote/[01;31m[K22[m[K470.c

Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)
| unix/remote/[01;31m[K22[m[K471.txt

Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Overflow
| unix/remote/[01;31m[K22[m[K356.c

Samba 3.5.[01;31m[K22[m[K/3.6.17/4.0.8 - nttrans Reply Integer Overflow
| linux/dos/27778.txt

Sambar Server 4.3/4.4 Beta 3 - Search CGI
| windows/remote/20[01;31m[K22[m[K3.txt

Sambar Server 5.1 - Sample Script Denial of Service
| windows/dos/21[01;31m[K22[m[K8.c

Sambar Server 5.x - 'results.stm' Cross-Site Scripting
| windows/remote/[01;31m[K22[m[K185.txt

Sambar Server 5.x - Information Disclosure
| windows/remote/[01;31m[K22[m[K434.txt

Sami HTTP Server 2.0.1 - GET Denial of Service
| windows/dos/154[01;31m[K22[m[K.pl

Samsung Kies 2.3.2.12054_20 - Multiple Vulnerabilities
| windows/remote/[01;31m[K22[m[K007.txt

Samsung SmartViewer BackupToAvi 3.0 - Remote Code Execution
| windows/remote/358[01;31m[K22[m[K.html

SAP Database 7.3/7.4 - SDBINST Race Condition
| linux/local/[01;31m[K22[m[K531.pl

SAP DB 7.3.00 - Symbolic Link
| unix/local/[01;31m[K22[m[K067.txt

Savant Web Server 3.1 - CGITest.HTML Cross-Site Scripting
| windows/remote/[01;31m[K22[m[K944.txt

Savant Web Server 3.1 - Denial of Service
| windows/dos/[01;31m[K22[m[K945.txt

Schneider Electric SBO / AS - Multiple Vulnerabilities
| hardware/remote/395[01;31m[K22[m[K.txt

School Event Management System 1.0 - SQL Injection
| php/webapps/457[01;31m[K22[m[K.txt

School Faculty Scheduling System 1.0 - Authentication Bypass POC
| php/webapps/489[01;31m[K22[m[K.txt

School Management System Pro 6.0.0 - Backup Dump
| asp/webapps/1[01;31m[K22[m[K18.txt

Schoolhos CMS Beta 2.29 - 'id' SQL Injection
| php/webapps/[01;31m[K22[m[K157.txt

ScozBook 1.1 - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K445.txt

Scripts4Profit DXShopCart 4.30 - 'pid' SQL Injection
| php/webapps/3[01;31m[K22[m[K83.txt

SDFingerD 1.1 - Failure To Drop Privileges Privilege Escalation
| linux/local/[01;31m[K22[m[K806.sh

Seat Reservation System 1.0 - 'id' SQL Injection
| php/webapps/488[01;31m[K22[m[K.txt

Secutech RiS-11/RiS-[01;31m[K22[m[K/RiS-33 - Remote DNS Change
| hardware/webapps/44393.sh

SeedDMS versions < 5.1.11 - Remote Command Execution
| php/webapps/470[01;31m[K22[m[K.txt

Sefrengo CMS 1.6.0 - SQL Injection
| php/webapps/357[01;31m[K22[m[K.txt

SEGGER embOS/IP FTP Server 3.[01;31m[K22[m[K - Denial of Service
| windows/dos/44[01;31m[K22[m[K1.py

SEIG Modbus 3.4 - Remote Code Execution
| windows_x86/remote/45[01;31m[K22[m[K0.py

Sendmail 8.11.6 - Address Prescan Memory Corruption
| unix/local/[01;31m[K22[m[K442.c

Sendmail 8.12.x - Header Processing Buffer Overflow (1)
| unix/remote/[01;31m[K22[m[K313.c

Sendmail 8.12.x - Header Processing Buffer Overflow (2)
| unix/remote/[01;31m[K22[m[K314.c

SePortal 2.5 - SQL Injection (1)
| php/webapps/18[01;31m[K22[m[K2.txt

Sera 1.2 - Local Privilege Escalation / Password Disclosure
| macos/local/43[01;31m[K22[m[K1.sh

Serenity Audio Player Playlist - '.m3u' Local Buffer Overflow
| windows/local/10[01;31m[K22[m[K6.py

SFS EZ Webstore - 'where' SQL Injection
| php/webapps/69[01;31m[K22[m[K.txt

SGI IRIX 5.x/6.x - Objectserver
| irix/remote/198[01;31m[K22[m[K.c

SGI IRIX 6.5.[01;31m[K22[m[K - GR_OSView Information Disclosure
| irix/local/25361.txt

SGI IRIX 6.5.[01;31m[K22[m[K - GR_OSView Local Arbitrary File Overwrite
| irix/local/25362.txt

Shadows Rising RPG 0.0.5b - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K29.txt

Shawn Bradley PHP Volunteer Management 1.0.2 - 'id' SQL Injection
| php/webapps/371[01;31m[K22[m[K.txt

SheerDNS 1.0 - Information Disclosure
| linux/remote/[01;31m[K22[m[K485.c

Shipping System CMS 1.0 - SQL Injection
| php/webapps/447[01;31m[K22[m[K.txt

SHTTPD 1.38 - Filename Parse Error Information Disclosure
| multiple/remote/30[01;31m[K22[m[K9.txt

siemens automation license manager 500.0.1[01;31m[K22[m[K.1 - Multiple
Vulnerabilities |
windows/dos/18165.txt

Siemens C450IP/C475IP - Remote Denial of Service
| hardware/dos/7[01;31m[K22[m[K0.txt

SIEMENS Sipass Integrated 2.6 Ethernet Bus - Arbitrary Pointer
Dereference |
windows/dos/[01;31m[K22[m[K397.txt

siemens tecnomatix factorylink 8.0.1.1473 - Multiple Vulnerabilities
| windows/remote/170[01;31m[K22[m[K.txt

SIESTTA 2.0 - Local File Inclusion / Cross-Site Scripting
| php/webapps/1[01;31m[K22[m[K60.txt

silentthought simple Web server 1.0 - Directory Traversal
| windows/remote/[01;31m[K22[m[K758.txt

SilverStripe CMS 2.4.5 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/36[01;31m[K22[m[K6.txt

```
Simasy CMS - 'id' SQL Injection
| php/webapps/3[01;31m[K22[m[K84.txt

SimpGB 1.0 - 'Guestbook.php' SQL Injection
| php/webapps/25[01;31m[K22[m[K4.txt

Simple Chat 1.x - User Information Disclosure
| multiple/remote/[01;31m[K22[m[K409.txt

Simple Machines Forum (SMF) 1.1 rc2 (Windows) - 'lngfile' Local File
Inclusion                               |
php/webapps/[01;31m[K22[m[K31.php

Simple Machines Forum (SMF) 1.1 rc2 - Lock Topics
| php/webapps/[01;31m[K22[m[K43.php

Simple Phone Book  1.0 - 'Username' SQL Injection (Unauthenticated)
| php/webapps/50[01;31m[K22[m[K3.txt

Simple Subscription Website 1.0 - SQLi Authentication Bypass
| php/webapps/505[01;31m[K22[m[K.txt

Simple Web Server 0.5.1 - File Disclosure
| windows/remote/[01;31m[K22[m[K001.txt

SimpleBBS 1.0.6 - 'users.php' Insecure File Permissions
| php/webapps/[01;31m[K22[m[K339.txt

SimpleBlog 2.0 - 'comments.asp' SQL Injection (1)
| asp/webapps/[01;31m[K22[m[K28.txt

SimpleBlog 2.0 - 'comments.asp' SQL Injection (2)
| php/webapps/[01;31m[K22[m[K32.pl

SimpleBlog 2.3 - 'id' SQL Injection
| asp/webapps/[01;31m[K22[m[K96.txt

SimpNews 2.0.1/2.13 - 'path_simpnews' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K927.txt

SIPS 0.2.2 - User Information Disclosure
| multiple/remote/[01;31m[K22[m[K381.txt

Sisfokol 4.0 - Arbitrary File Upload
| php/webapps/[01;31m[K22[m[K038.txt

Siteframe CMS 2.2.4 - 'download.php' Information Disclosure
| php/webapps/[01;31m[K22[m[K386.txt

SiteGo - Remote File Inclusion
| php/webapps/21[01;31m[K22[m[K2.txt
```

```
SkaDate - 'blogs.php' Cross-Site Scripting
| php/webapps/361[01;31m[K22[m[K.txt

Slackware Linux 3.5 - '/etc/group' Local Privilege Escalation
| linux/local/191[01;31m[K22[m[K.txt

sleuthkit 4.11.1 - Command Injection
| multiple/local/51[01;31m[K22[m[K5.txt

slocate 2.5/2.6 - Local Buffer Overrun
| linux/dos/[01;31m[K22[m[K197.txt

SLocate 2.6 - User-Supplied Database Heap Overflow
| linux/local/23[01;31m[K22[m[K8.c

Smadav Anti Virus 9.1 - Crash (PoC)
| windows/dos/[01;31m[K22[m[K653.py

Smart Manager 8.27.0 - Post-Authenticated SQL Injection
| php/webapps/5[01;31m[K22[m[K47.txt

Smart Search 4.25 - Remote Command Execution
| cgi/webapps/[01;31m[K22[m[K380.pl

Smart Survey 1.0 - 'surveyresults.asp' Cross-Site Scripting
| asp/webapps/3[01;31m[K22[m[K97.txt

SmartCMS - 'index.php?idx' SQL Injection
| php/webapps/[01;31m[K22[m[K936.txt

SmartDesk WebSuite 2.1 - Remote Buffer Overflow
| multiple/remote/19[01;31m[K22[m[K1.txt

SmarterTools SmarterTrack 79[01;31m[K22[m[K - 'Multiple' Information
Disclosure                                          |
aspx/webapps/50328.txt

Smoothflash - 'cid' SQL Injection
| php/webapps/53[01;31m[K22[m[K.txt

Snitz Forums 2000 - 'register.asp' SQL Injection
| asp/webapps/[01;31m[K22[m[K583.pl

Snitz Forums 2000 3.4.03 - 'search.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K22[m[K778.txt

Snowblind 1.0/1.1 - Web Server File Disclosure
| windows/remote/[01;31m[K22[m[K609.txt

Snowblind Web Server 1.0/1.1 - GET Buffer Overflow
| windows/dos/[01;31m[K22[m[K610.txt
```

Snowblind Web Server 1.0/1.1 - Malformed HTTP Request Denial of Service
| windows/dos/[01;31m[K22[m[K608.txt

SNScan 1.05 - Scan Hostname/IP Field Buffer Overflow Crash (PoC)
| windows/dos/39[01;31m[K22[m[K6.py

Social Share - 'postid' SQL Injection
| php/webapps/351[01;31m[K22[m[K.txt

Softbiz B2B trading Marketplace Script - buyers_subcategories SQL
Injection |
php/webapps/1[01;31m[K22[m[K45.txt

Softrex Tornado WWW-Server 1.2 - Buffer Overflow
| windows/dos/[01;31m[K22[m[K666.txt

Softshoe - Parse-file Cross-Site Scripting
| cgi/webapps/[01;31m[K22[m[K963.txt

Software602 602 Lan Suite 2004 2004.0.04.1[01;31m[K22[m[K1 - Arbitrary
File Upload |
windows/remote/25092.txt

Solaris 10 sysinfo(2) - Local Kernel Memory Disclosure (2)
| solaris/local/[01;31m[K22[m[K41.c

Solaris 8/9 - '/usr/ucb/ps' Local Information Leak
| solaris/local/[01;31m[K22[m[K42.sh

Solaris 8/9/10 - 'fifofs I_PEEK' Local Kernel Memory Leak
| solaris/local/5[01;31m[K22[m[K7.c

Solaris LPD - Command Execution (Metasploit)
| solaris/remote/163[01;31m[K22[m[K.rb

SonicWALL Aventail SSL-VPN - SQL Injection
| hardware/webapps/181[01;31m[K22[m[K.txt

SonicWALL CDP 5040 6.x - Multiple Vulnerabilities
| multiple/webapps/[01;31m[K22[m[K852.txt

SonicWALL Gms 6 - Arbitrary File Upload (Metasploit)
| multiple/remote/243[01;31m[K22[m[K.rb

Sonium Enterprise Adressbook 0.2 - 'folder' Include
| php/webapps/[01;31m[K22[m[K16.txt

Sony Playstation 4 (PS4) < 6.20 - WebKit Code Execution (PoC)
| hardware/local/465[01;31m[K22[m[K.md

SOOP Portal Raven 1.0b - SQL Injection
| asp/webapps/17[01;31m[K22[m[K8.txt

```
Sophos Products - Multiple Vulnerabilities
| multiple/remote/[01;31m[K22[m[K509.txt

South River Technologies WebDrive 9.02 build [01;31m[K22[m[K32 - Local
Privilege Escalation                              |
windows/local/9970.txt

South River Technologies WebDrive Service 9.02 build [01;31m[K22[m[K32
- Bad Security Descriptor Privilege Escalation   |
windows/local/11264.rb

SPChat 0.8 Module - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K717.txt

SPGPartenaires 3.0.1 - 'delete.php' SQL Injection
| php/webapps/[01;31m[K22[m[K108.txt

SPGPartenaires 3.0.1 - 'ident.php' SQL Injection
| php/webapps/[01;31m[K22[m[K107.txt

Sphera HostingDirector 1.0/2.0/3.0 - VDS Control Panel Account
Configuration Modification                  |
php/webapps/[01;31m[K22[m[K760.txt

Sphera HostingDirector 1.0/2.0/3.0 VDS Control Panel - Multiple Cross-
Site Scripting Vulnerabilities       |
php/webapps/[01;31m[K22[m[K762.txt

SPIP CMS < 2.0.23/ 2.1.[01;31m[K22[m[K/3.0.9 - Privilege Escalation
| php/webapps/33425.py

Spitfire 1.0.3x - 'cms_username' Cross-Site Scripting
| php/webapps/355[01;31m[K22[m[K.txt

Splatt Forum 3/4 - Post Icon HTML Injection
| php/webapps/[01;31m[K22[m[K910.html

Splunk 5.0 - Custom App Remote Code Execution (Metasploit)
| multiple/remote/23[01;31m[K22[m[K4.rb

SportsPHool 1.0 - 'mainnav' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K27.txt

SpotPaltalk 1.1.5 - Denial of Service (PoC)
| windows/dos/468[01;31m[K22[m[K.py

Spring Boot common-user-management 0.1 - Remote Code Execution (RCE)
| java/webapps/5[01;31m[K22[m[K06.py

SpyCamLizard 1.230 - Remote Buffer Overflow
| windows/remote/4[01;31m[K22[m[K[01;31m[K22[m[K.py
```

```
SquirrelMail 1.2.11 - 'move_messages.php' Arbitrary File Moving
| php/webapps/[01;31m[K22[m[K791.txt

SquirrelMail 1.2.11 - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K793.txt

SquirrelMail 1.2.11 Administrator Plugin - 'options.php' Arbitrary
Admin Account Creation                  |
php/webapps/[01;31m[K22[m[K792.txt

SquirrelMail < 1.4.[01;31m[K22[m[K - Remote Code Execution
| linux/remote/41910.sh

SqWebMail 4.0.4.20040524 - Email Header HTML Injection
| php/webapps/24[01;31m[K22[m[K7.txt

StarSiege Tribes Server - Denial of Service (1)
| windows/dos/[01;31m[K22[m[K899.txt

StarSiege Tribes Server - Denial of Service (2)
| windows/dos/[01;31m[K22[m[K900.php

Steamcast - HTTP Request Remote Buffer Overflow (SEH) (2)
| windows/remote/84[01;31m[K22[m[K.py

StivaSoft Stiva SHOPPING CART 1.0 - 'demo.php' Cross-Site Scripting
| php/webapps/340[01;31m[K22[m[K.txt

Stockman Shopping Cart 7.8 - Arbitrary Command Execution
| cgi/webapps/[01;31m[K22[m[K559.pl

Streamripper 1.61.25 - HTTP Header Parsing Buffer Overflow (1)
| linux/remote/[01;31m[K22[m[K74.c

Streamripper 1.61.25 - HTTP Header Parsing Buffer Overflow (2)
| windows/remote/[01;31m[K22[m[K77.c

Subberz Lite - UserFunc Remote File Inclusion
| php/webapps/28[01;31m[K22[m[K3.txt

subrion CMS 2.2.1 - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K159.txt

Subtitle Processor 7.7.1 - '.m3u' File Buffer Overflow (SEH Unicode)
(Metasploit)                            |
windows/local/17[01;31m[K22[m[K5.rb

SudBox Boutique 1.2 - 'login.php' Authentication Bypass
| php/webapps/[01;31m[K22[m[K625.txt

Sudo 1.6.3 - Unclean Environment Variable Privilege Escalation
| linux/local/21[01;31m[K22[m[K7.sh
```

Sudo 1.9.5p1 - 'Baron Samedit ' Heap-Based Buffer Overflow Privilege Escalation (2) | multiple/local/495[01;31m[K22[m[K.c

SUIDPerl 5.6 - Information Disclosure | linux/local/[01;31m[K22[m[K055.txt

Sun HotJava Browser 3 - Arbitrary DOM Access | multiple/remote/203[01;31m[K22[m[K.html

Sun JDK/SDK 1.3/1.4 / IBM JDK 1.3.1 / BEA Systems WebLogic 5/6/7 - java.util.zip Null Value Denial of Serv | multiple/dos/[01;31m[K22[m[K358.cfm

Sun JDK/SDK 1.3/1.4 / IBM JDK 1.3.1 / BEA Systems WebLogic 5/6/7 - java.util.zip Null Value Denial of Serv | multiple/dos/[01;31m[K22[m[K359.xsl

Sun JDK/SDK 1.3/1.4 / IBM JDK 1.3.1 / BEA Systems WebLogic 5/6/7 - java.util.zip Null Value Denial of Serv | multiple/dos/[01;31m[K22[m[K360.java

Sun JRE/SDK 1.x - Untrusted Applet Java Security Model Violation | multiple/local/[01;31m[K22[m[K732.java

Sun One 5.1 / IPlanet 5.0/5.1 - Administration Server Directory Traversal | multiple/remote/[01;31m[K22[m[K994.txt

Sun ONE Application Server 7.0 - Error Message Cross-Site Scripting | windows/remote/[01;31m[K22[m[K665.txt

Sun ONE Application Server 7.0 - Source Disclosure | windows/remote/[01;31m[K22[m[K664.txt

Sun ONE Unified Development Server 5.0 - Recursive Document Type Definition | multiple/remote/[01;31m[K22[m[K178.xml

Sun Solaris 2.5.1/2.6/7.0/8/9 Wall - Spoofed Message Origin | solaris/local/[01;31m[K22[m[K120.c

Sun Solaris 2.5/2.6/7.0/8/9 AT Command - Arbitrary File Deletion | solaris/local/[01;31m[K22[m[K203.txt

Sun/Netscape Java Virtual Machine1.x - Bytecode Verifier | multiple/remote/[01;31m[K22[m[K029.txt

Sunbelt Kerio Personal Firewall 4.3.426 - CreateRemoteThread Denial of Service | hardware/dos/28[01;31m[K22[m[K8.txt

Super Guestbook 1.0 - Sensitive Information Disclosure
| cgi/webapps/[01;31m[K22[m[K481.txt

SuperBackup 2.0.5 for iOS - Persistent Cross-Site Scripting
| ios/webapps/483[01;31m[K22[m[K.txt

SuperStoreFinder - Multiple Vulnerabilities
| php/webapps/518[01;31m[K22[m[K.txt

SureTriggers OttoKit Plugin 1.0.82 - Privilege Escalation
| multiple/webapps/5[01;31m[K22[m[K86.txt

SurfControl Web Filter 4.2.0.1 - File Disclosure
| windows/remote/[01;31m[K22[m[K807.txt

Survey Sparrow Enterprise Survey Software 20[01;31m[K22[m[K - Stored
Cross-Site Scripting (XSS) |
multiple/webapps/50937.txt

SuSE Linux Professional 8.2 - SuSEWM Configuration File Insecure
Temporary File |
linux/local/23[01;31m[K22[m[K3.c

SyGate 5.0 - Insecure UDP Source Port Firewall Bypass Weak Default
Configuration |
multiple/remote/[01;31m[K22[m[K200.txt

Symantec Java! JustInTime Compiler 210.65 - Command Execution
| windows/remote/[01;31m[K22[m[K028.txt

Symantec Messaging Gateway 10.6.2-7 - Remote Code Execution
(Metasploit) |
python/remote/4[01;31m[K22[m[K51.rb

Symantec Norton AntiVirus 2002/2003 - Device Driver Memory Overwrite
| windows/local/[01;31m[K22[m[K980.asm

Symantec Norton Internet Security 2003 - ICMP Packet Flood Denial of
Service |
windows/dos/[01;31m[K22[m[K162.txt

Symantec Security Check RuFSI - ActiveX Control Buffer Overflow
| windows/dos/[01;31m[K22[m[K816.txt

Symphony CMS 2.3 - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K039.txt

Synkron.Web 3.0 - HTML Injection
| asp/webapps/[01;31m[K22[m[K744.txt

Synology DSM 4.3-3827 - 'article.php' Blind SQL Injection
| php/webapps/3[01;31m[K22[m[K74.txt

SysAid Help Desk Software 14.4.32 b25 - SQL Injection (Metasploit)
| windows/webapps/388[01;31m[K22[m[K.rb

Sysax FTP Automation Server 5.33 - Local Privilege Escalation
| windows/local/[01;31m[K22[m[K465.txt

System CMS Contentia - 'news.php' SQL Injection
| php/webapps/34[01;31m[K22[m[K6.txt

Systemd [01;31m[K22[m[K8 (SUSE 12 SP2 / Ubuntu Touch 15.04) - Local Privilege Escalation |
linux/local/41171.txt

TABS MailCarrier 2.51 - SMTP EHLO Overflow (Metasploit)
| windows/remote/168[01;31m[K22[m[K.rb

Talkative IRC 0.4.4.16 - Remote Stack Overflow (SEH)
| windows/remote/8[01;31m[K22[m[K7.pl

TANne 0.6.17 - Session Manager SysLog Format String
| linux/remote/[01;31m[K22[m[K135.c

tar-fs 3.0.0 - Arbitrary File Write/Overwrite
| linux/local/5[01;31m[K22[m[K68.py

Task Management System 1.0 - 'First Name and Last Name' Stored XSS
| php/webapps/49[01;31m[K22[m[K2.txt

Task Management System 1.0 - 'id' SQL Injection
| php/webapps/49[01;31m[K22[m[K4.txt

Task Management System 1.0 - Unrestricted File Upload to Remote Code Execution |
php/webapps/49[01;31m[K22[m[K3.txt

Tatsu 3.3.11 - Unauthenticated RCE
| php/webapps/5[01;31m[K22[m[K60.py

TCPDump 3.6/3.7 - Malformed RADIUS Packet Denial of Service
| linux/dos/[01;31m[K22[m[K352.txt

TCPDump 3.x - Malformed ISAKMP Packet Denial of Service
| linux/dos/[01;31m[K22[m[K294.c

Tdarr 2.00.15 - Command Injection
| multiple/remote/508[01;31m[K22[m[K.txt

Technote 2000/2001 - 'board' File Disclosure
| cgi/remote/205[01;31m[K22[m[K.txt

Teedy 1.11 - Account Takeover via Stored Cross-Site Scripting (XSS)
| multiple/webapps/5[01;31m[K22[m[K28.txt

```
Telekorn Signkorn Guestbook 1.x - 'index.php?dir_path' Remote File
Inclusion                                |
php/webapps/285[01;31m[K22[m[K.txt

TestLink Open Source Test Management < 1.9.16 - Remote Code Execution
| php/remote/44[01;31m[K22[m[K6.txt

Texas Imperial Software WFTPD 3.23 - 'SIZE' Remote Buffer Overflow
| windows/remote/[01;31m[K22[m[K33.c

TFTPD32 2.50 - 'Filename' Remote Buffer Overflow
| windows/remote/[01;31m[K22[m[K025.pl

TFTPD32 2.50 - Arbitrary File Download/Upload
| windows/remote/[01;31m[K22[m[K024.txt

TGS Content Management 0.3.2r2 - 'index.php' Multiple Cross-Site
Scripting Vulnerabilities                |
php/webapps/320[01;31m[K22[m[K.txt

The Includer CGI 1.0 - Remote Command Execution (2)
| cgi/webapps/9[01;31m[K22[m[K.pl

Thunderstone TEXIS 3.0 - 'texis.exe' Information Disclosure
| cgi/remote/[01;31m[K22[m[K355.txt

Tibco ObfuscationEngine 5.11 - Fixed Key Password Decryption
| multiple/local/49[01;31m[K22[m[K1.java

TIBCO Rendezvous 7.4.11 - add router Remote Buffer Overflow
| windows/remote/[01;31m[K22[m[K83.c

TIBCO Rendezvous 7.4.11 - Password Extractor
| windows/local/[01;31m[K22[m[K84.c

TightVNC 2.8.83 - Control Pipe Manipulation
| multiple/local/523[01;31m[K22[m[K.c

TikiWiki 1.9 Sirius - 'jhot.php' Remote Command Execution
| php/webapps/[01;31m[K22[m[K88.php

TildeSlash Monit 1-4 - Authentication Handling Buffer Overflow
| multiple/remote/24[01;31m[K22[m[K4.c

TimeTrex Time 2.2 and Attendance Module - Multiple Cross-Site Scripting
Vulnerabilities                  | php/webapps/3[01;31m[K22[m[K88.txt

TinyPHPForum 3.6 - 'error.php' Information Disclosure
| php/webapps/283[01;31m[K22[m[K.txt

TinyWebGallery 1.8.3 - Remote Command Execution
| php/webapps/183[01;31m[K22[m[K.txt
```

```
TIPS MailPost 5.1.1 - Error Message Cross-Site Scripting
| cgi/webapps/247[01;31m[K22[m[K.txt

TipsOfTheDay MyBB Plugin - Multiple Vulnerabilities
| php/webapps/233[01;31m[K22[m[K.txt

Tmax Soft JEUS 3.1.4 p1 - URL.jsp Cross-Site Scripting
| jsp/webapps/[01;31m[K22[m[K805.txt

Tolis Group BRU 17.0 - Local Privilege Escalation (1)
| unix/local/[01;31m[K22[m[K923.c

Tolis Group BRU 17.0 - Local Privilege Escalation (2)
| unix/local/[01;31m[K22[m[K924.c

Tomabo MP4 Converter 3.25.[01;31m[K22[m[K - Denial of Service (PoC)
| windows/dos/46848.py

Top 1.x/2.0 - 'HOME Environment' Local Buffer Overflow
| linux/local/[01;31m[K22[m[K943.c

TopList 1.3.8 - 'phpBB Hack' Remote File Inclusion (1)
| php/webapps/17[01;31m[K22[m[K.txt

TOPO 1.41 - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K[01;31m[K22[m[K2.txt

TornadoStore 1.4.3 - SQL Injection / HTML Injection
| php/webapps/34[01;31m[K22[m[K5.txt

Tower Toppler 0.96 - 'HOME Environment' Local Buffer Overflow
| linux/local/[01;31m[K22[m[K884.c

Tower Toppler 0.99.1 - 'Display' Local Buffer Overflow
| unix/local/[01;31m[K22[m[K335.pl

TP-Link Archer C50 Wireless Router 171[01;31m[K22[m[K7 - Cross-Site
Request Forgery (Configuration File Disclosure)     |
hardware/webapps/45811.rb

TP-Link NC200/NC[01;31m[K22[m[K0 Cloud Camera 300Mbps Wi-Fi - Hard-
Coded Credentials                                   |
hardware/remote/38186.txt

TP-Link TL-MR3[01;31m[K22[m[K0 - Cross-Site Scripting
| hardware/webapps/43023.txt

TP-Link VN020 F3v(T) TT_V6.2.1021 - Buffer Overflow Memory Corruption
| multiple/remote/5[01;31m[K22[m[K49.c

TP-Link VN020 F3v(T) TT_V6.2.1021 - Denial Of Service (DOS)
| multiple/remote/5[01;31m[K22[m[K50.txt
```

TP-Link VN020 F3v(T) TT_V6.2.1021) - DHCP Stack Buffer Overflow
| multiple/local/5[01;31m[K22[m[K92.c

TP-Link WR940N - (Authenticated) Remote Code
| hardware/webapps/430[01;31m[K22[m[K.py

TR Forum 2.0 - SQL Injection / Bypass Security Restriction
| php/webapps/[01;31m[K22[m[K97.pl

Traceroute-nanog 6 - Local Buffer Overflow
| linux/local/[01;31m[K22[m[K014.c

Trend Micro Deep Discovery Inspector 3.8/3.7 - Cross-Site Request Forgery |
hardware/webapps/396[01;31m[K22[m[K.txt

Trend Micro Internet Security Pro 2009 - Priviliege Escalation
| windows/local/83[01;31m[K22[m[K.txt

Trend Micro OfficeScan 3.x - CGI Directory Insufficient Permissions
| windows/remote/[01;31m[K22[m[K171.txt

Trend Micro PC-cillin 2000/2002/2003 - Mail Scanner Buffer Overflow
| windows/remote/[01;31m[K22[m[K082.pl

Trend Micro ScanMail For Exchange 3.8 - Authentication Bypass
| windows/remote/[01;31m[K22[m[K174.txt

Trend Micro Virus Control System 1.8 - Denial of Service
| windows/dos/[01;31m[K22[m[K172.txt

Trend Micro Virus Control System 1.8 - Information Disclosure
| windows/remote/[01;31m[K22[m[K173.txt

TRENDnet SecurView Wireless Network Camera TV-IP4[01;31m[K22[m[KWN - 'UltraCamX.ocx' Stack Buffer Overflow (PoC) |
windows/dos/35363.txt

Tripbit Secure Code Analizer 1.0 - 'fgets()' Local Buffer Overrun
| windows/local/[01;31m[K22[m[K835.c

TrouSerS - Denial of Service
| linux/dos/[01;31m[K22[m[K904.py

Truegalerie 1.0 - Unauthorized Administrative Access
| php/webapps/[01;31m[K22[m[K534.txt

ttCMS 2.2 / ttForum 1.1 - 'install.php?installdir' Remote File Inclusion |
php/webapps/[01;31m[K22[m[K578.txt

ttCMS 2.2 / ttForum 1.1 - 'news.php?template' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K577.txt

```
ttCMS 2.2/2.3 - 'header.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K612.txt

ttCMS 2.2/2.3 / ttForum 1.1 - 'index.php' Instant-Messages Preferences
SQL Injection                         |
php/webapps/[01;31m[K22[m[K618.txt

Turbo FTP Server 1.30.823 - PORT Overflow (Metasploit)
| windows/remote/[01;31m[K22[m[K161.rb

TurboTrafficTrader C 1.0 - Multiple Cross-Site Scripting / HTML
Injection Vulnerabilities                   |
cgi/webapps/241[01;31m[K22[m[K.txt

Tutos 1.1 - 'File_Select.php' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K818.txt

Tutos 1.1 - File_New Arbitrary File Upload
| php/webapps/[01;31m[K22[m[K819.txt

Tutti Nova 1.6 - 'TNLIB_DIR' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K20.txt

TuttoPHP Morris Guestbook - 'view.php' Cross-Site Scripting
| php/webapps/33[01;31m[K22[m[K7.txt

TW-WebServer 1.0 - Denial of Service (1)
| multiple/dos/[01;31m[K22[m[K502.pl

TW-WebServer 1.0 - Denial of Service (2)
| multiple/dos/[01;31m[K22[m[K503.c

TweakFS 1.0 FSX Edition - Stack Buffer Overflow
| windows/local/1[01;31m[K22[m[K93.py

Twilight WebServer 1.3.3.0 - GET Buffer Overflow
| linux/dos/[01;31m[K22[m[K897.c

txtSQL 2.2 Final - 'startup.php' Remote File Inclusion
| php/webapps/6[01;31m[K22[m[K4.txt

Typo3 3.5 b5 - 'showpic.php' File Enumeration
| php/webapps/[01;31m[K22[m[K297.pl

Typo3 3.5 b5 - 'Translations.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K298.txt

Typo3 3.5 b5 - HTML Hidden Form Field Information Disclosure (1)
| php/webapps/[01;31m[K22[m[K315.pl

Typo3 3.5 b5 - HTML Hidden Form Field Information Disclosure (2)
| php/webapps/[01;31m[K22[m[K316.pl
```

TYPSoft FTP Server 0.7.x - FTP Server Remote Denial of Service
| windows/dos/20[01;31m[K22[m[K8.pl

TYPSoft FTP Server 1.10 - APPE DELE Denial of Service
| windows/dos/10[01;31m[K22[m[K3.txt

UADMIN Botnet 1.0 - 'link' SQL Injection
| php/webapps/48[01;31m[K22[m[K2.txt

UApplication Uguestbook 1.0 - 'index.asp' SQL Injection
| asp/webapps/29[01;31m[K22[m[K4.txt

Ubee EVW3200 - Cross-Site Request Forgery
| hardware/webapps/3[01;31m[K22[m[K38.txt

Ubee EVW3200 - Multiple Persistent Cross-Site Scripting Vulnerabilities
| hardware/webapps/3[01;31m[K22[m[K37.txt

Ubee EVW3[01;31m[K22[m[K6 Modem/Router 1.0.20 - Multiple
Vulnerabilities |
cgi/webapps/40156.py

UFO: Alien Invasion 2.2.1 (Windows 7) - Remote Buffer Overflow (ASLR +
DEP Bypass) |
windows/remote/14[01;31m[K22[m[K2.py

UJCMS 9.6.3 - User Enumeration via IDOR
| multiple/webapps/5[01;31m[K22[m[K64.py

Ultimate Bulletin Board 6.0/6.2 - UBBER Cookie HTML Injection
| php/webapps/[01;31m[K22[m[K9[01;31m[K22[m[K.txt

Ultimate PHP Board 1.0 final Beta - 'viewtopic.php' Directory Contents
Browsing |
php/webapps/[01;31m[K22[m[K075.txt

Ultimate PHP Board 1.9 - 'admin_iplog.php' Arbitrary PHP Execution
| php/webapps/[01;31m[K22[m[K642.txt

Ultimate PHP Board Board 1.0 final Beta - 'viewtopic.php' Cross-Site
Scripting |
php/webapps/[01;31m[K22[m[K076.txt

UltraPlayer 2.112 - '.avi' File Denial of Service
| windows/dos/366[01;31m[K22[m[K.pl

UML_NET - Integer Mismanagement Code Execution
| linux/local/[01;31m[K22[m[K640.c

UNA 10.0.0 RC1 - 'polyglot.php' Persistent Cross-Site Scripting
| php/webapps/47[01;31m[K22[m[K1.txt

```
Unclassified NewsBoard 1.5.3 - 'Description' HTML Injection
| php/webapps/26[01;31m[K22[m[K4.txt

Unified Office Total Connect Now 1.0 - 'data' SQL Injection
| php/webapps/500[01;31m[K22[m[K.txt

University of Minnesota Gopherd 2.0.x/2.3/3.0.x - FTP Gateway Buffer
Overflow                                  |
linux/remote/[01;31m[K22[m[K893.c

University of Minnesota Gopherd 2.0.x/2.3/3.0.x - GSisText Buffer
Overflow                                    |
linux/remote/[01;31m[K22[m[K894.c

University of Washington pop2d 4.4 - Remote Buffer Overflow
| linux/remote/19[01;31m[K22[m[K6.c

unrar 5.40 - 'VMSF_DELTA' Filter Arbitrary Memory Write
| multiple/dos/4[01;31m[K22[m[K45.txt

UnrealIRCd 3.2.8.1 - Backdoor Command Execution (Metasploit)
| linux/remote/169[01;31m[K22[m[K.rb

unzip-stream 0.3.1 - Arbitrary File Write
| nodejs/local/5[01;31m[K22[m[K76.py

Upclient 5.0 b7 - Command Line Argument Buffer Overflow
| freebsd/local/[01;31m[K22[m[K661.c

Uploader 0.7 - Arbitrary File Upload
| php/webapps/1[01;31m[K22[m[K68.txt

URLStreet 1.0 - 'seeurl.php' Multiple Cross-Site Scripting
Vulnerabilities                                  |
php/webapps/316[01;31m[K22[m[K.txt

Usermin 2.100 - Username Enumeration
| multiple/webapps/5[01;31m[K22[m[K54.py

uWSGI < 2.0.17 - Directory Traversal
| php/webapps/44[01;31m[K22[m[K3.txt

V-Webmail 1.6.4 -
'/includes/pear/Mail/RFC8[01;31m[K22[m[K.php?CONFIG[pear_dir]' Remote
File Inclusion                  | php/webapps/32024.txt

Vacation Rental Script 3.0 - 'id' SQL Injection
| php/webapps/6[01;31m[K22[m[K1.txt

Valve Software Half-Life 1.1 Client - Connection Routine Buffer
Overflow (1)                                  |
windows/remote/[01;31m[K22[m[K966.c
```

```
Valve Software Half-Life 1.1 Client - Connection Routine Buffer
Overflow (2)                                  |
windows/remote/[01;31m[K22[m[K967.txt

Valve Software Half-Life Server 1.1.1.0/3.1.1.1c1/4.1.1.1a -
Multiplayer Request Buffer Overflow           |
linux/remote/[01;31m[K22[m[K968.c

Valve Software Half-Life Server 3.1.1.0 - Multiplayer Request Buffer
Overflow                                      |
linux/remote/[01;31m[K22[m[K969.c

vam shop 1.69 - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K372.txt

Vanilla 1.1.4 - HTML Injection / Cross-Site Scripting
| php/webapps/3[01;31m[K22[m[K79.txt

vAuthenticate 2.8 - SQL Injection
| php/webapps/[01;31m[K22[m[K167.txt

VBox Satellite Express 2.3.17.3 - Arbitrary Write
| windows/dos/38[01;31m[K22[m[K5.txt

VBScript - VbsErase Reference Leak Use-After-Free
| windows/dos/460[01;31m[K22[m[K.txt

vBulletin 2.0.x/2.2.x - 'members2.php' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K042.php

vBulletin 2.0/2.2.x - 'memberlist.php' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K030.php

vBulletin 2.2.7/2.2.8 - HTML Injection
| php/webapps/[01;31m[K22[m[K077.txt

vBulletin 3.0 - 'forumdisplay.php' Cross-Site Scripting
| php/webapps/238[01;31m[K22[m[K.txt

vBulletin 3.0 - 'register.php' HTML Injection
| php/webapps/[01;31m[K22[m[K990.txt

vBulletin 3.0 - Private Message HTML Injection
| php/webapps/[01;31m[K22[m[K599.html

vBulletin 3.6.10/3.7.2 - '$newpm[title]' Cross-Site Scripting
| php/webapps/3[01;31m[K22[m[K85.txt

vBulletin 5.2.2 - Server-Side Request Forgery
| php/webapps/40[01;31m[K22[m[K5.py

vBulletin ChangUonDyU Advanced Statistics - SQL Injection
| php/webapps/[01;31m[K22[m[K429.txt
```

```
vBulletin vBay 1.1.9 - Error-Based SQL Injection
| php/webapps/[01;31m[K22[m[K656.py

vCard PRO - 'search.php?event_id' SQL Injection
| php/webapps/281[01;31m[K22[m[K.txt

Verilink NetEngine 6100-4 Broadband Router - TFTP Packet Remote Denial
of Service                          |
hardware/dos/[01;31m[K22[m[K596.txt

Veritas/Symantec Backup Exec - SSL NDMP Connection Use-After-Free
(Metasploit)                                |
windows/remote/4[01;31m[K22[m[K82.rb

Verity K2 Toolkit 2.20 - Cross-Site Scripting
| jsp/webapps/[01;31m[K22[m[K849.txt

Verity K2 Toolkit 2.20 Query Builder Search Script - Cross-Site
Scripting                                    |
jsp/webapps/[01;31m[K22[m[K857.txt

VestaCP 0.9.8-26 - 'backup' Information Disclosure
| multiple/webapps/49[01;31m[K22[m[K0.txt

Vestel TV 42pf93[01;31m[K22[m[K - Denial of Service
| hardware/dos/28271.py

VFU 4.10-1.1 - Move Entry Buffer Overflow
| linux/local/36[01;31m[K22[m[K9.py

VHCS 2.4.7.1 - 'vhcs2_daemon' Remote Code Execution
| linux/remote/5[01;31m[K22[m[K4.php

ViArt CMS/Shop/Helpdesk 3.3.2 - Remote File Inclusion
| php/webapps/47[01;31m[K22[m[K.txt

VICIDIAL Call Center Suite 2.2.1-237 - Multiple Vulnerabilities
| php/webapps/21[01;31m[K22[m[K0.txt

VideoDB 3.0.3 - Multiple Vulnerabilities
| php/webapps/15[01;31m[K22[m[K5.txt

VidiScript - SQL Injection
| php/webapps/16[01;31m[K22[m[K3.txt

Vignette 4.x/5.0 - Memory Disclosure
| unix/remote/[01;31m[K22[m[K646.txt

Vignette 4/5 - Cross-Site Scripting
| unix/remote/[01;31m[K22[m[K648.txt
```

Vignette StoryServer 4.1 - Sensitive Stack Memory Information Disclosure | multiple/remote/[01;31m[K22[m[K472.txt

Vikingboard 0.2 Beta - 'register.php' SQL Column Truncation Unauthorized Access | php/webapps/324[01;31m[K22[m[K.txt

Vim - 'mch_expand_wildcards()' Heap Buffer Overflow | linux/remote/3[01;31m[K22[m[K25.txt

Vim 7.1.314 - Insufficient Shell Escaping Multiple Command Execution Vulnerabilities | linux/remote/3[01;31m[K22[m[K89.txt

Viral Image Sharing Script - SQL Injection | php/webapps/411[01;31m[K22[m[K.txt

Virtual Programming VP-ASP 5.00 - 'shopexd.asp' SQL Injection (1) | asp/webapps/[01;31m[K22[m[K888.pl

Virtual Programming VP-ASP 5.00 - 'shopexd.asp' SQL Injection (2) | asp/webapps/[01;31m[K22[m[K889.pl

VirtualBox 5.1.[01;31m[K22[m[K - Windows Process DLL Signature Bypass Privilege Escalation | windows/local/42425.txt

VirtualBox 5.1.[01;31m[K22[m[K - Windows Process DLL UNC Path Signature Bypass Privilege Escalation | windows/local/42426.txt

VirtualBox 7.0.16 - Privilege Escalation | windows/local/5[01;31m[K22[m[K87.C++

Virtue Online Test Generator - Authentication Bypass / SQL Injection / Cross-Site Scripting | php/webapps/90[01;31m[K22[m[K.txt

VirusChaser 8.0 - Stack Buffer Overflow | windows/dos/325[01;31m[K22[m[K.py

VisNetic ActiveDefense 1.3.1 - GET Multiple Denial of Service Vulnerabilities | multiple/dos/[01;31m[K22[m[K535.txt

VisNetic Mail Server 8.3.5 - Multiple File Inclusions | php/webapps/28[01;31m[K22[m[K9.txt

VisNetic WebMail 5.8.6 .6 - Information Disclosure | php/webapps/[01;31m[K22[m[K826.txt

VistaBB 2.x - 'functions_mod_user.php' Remote File Inclusion | php/webapps/[01;31m[K22[m[K51.pl

Visual Tools DVR3.0.6.16_ vx series 4.2.19.2 - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K22[m[K005.txt

Vixie Cron crontab 3.0 - Privilege Lowering Failure (1)
| linux/local/208[01;31m[K22[m[K.sh

VMware 5.5.1 - 'ActiveX' Local Buffer Overflow
| windows/local/[01;31m[K22[m[K64.html

VocalTec VGW120/VGW480 Telephony Gateway Remote H.[01;31m[K22[m[K5 - Denial of Service |
hardware/dos/24143.c

VoteBox 2.0 - 'Votebox.php' Remote File Inclusion
| php/webapps/25[01;31m[K22[m[K6.txt

vPhoto-Album 4.2 iOS - Local File Inclusion
| ios/webapps/369[01;31m[K22[m[K.txt

VPOPMail 0.9x - 'vpopmail.php' Remote Command Execution
| php/webapps/[01;31m[K22[m[K343.txt

VS-News-System 1.2.1 - 'newsordner' Remote File Inclusion
| php/webapps/33[01;31m[K22[m[K.html

VSAXESS V2.6.2.70 build 20171[01;31m[K22[m[K6_053 - 'Nickname' Denial of Service (PoC) |
windows/dos/45315.py

VSAXESS V2.6.2.70 build20171[01;31m[K22[m[K6_053 - 'organization' Denial of Service (PoC) |
windows/dos/45800.py

vSignup 2.1 - SQL Injection
| php/webapps/[01;31m[K22[m[K168.txt

Vt-Forum Lite 1.3 - 'vf_info.asp?StrMes' Cross-Site Scripting
| asp/webapps/29[01;31m[K22[m[K7.txt

Vt-Forum Lite 1.3 - 'vf_newtopic.asp' IFRAME Element Cross-Site Scripting |
asp/webapps/29[01;31m[K22[m[K8.txt

vTiger CRM 5.4.0/6.0 RC/6.0.0 GA - 'browse.php' Local File Inclusion
| php/webapps/3[01;31m[K22[m[K13.txt

W-Agora 4.1.6 - 'EditForm.php' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K109.txt

W-Agora 4.1.6 - 'index.php?bn' Traversal Arbitrary File Access
| php/webapps/[01;31m[K22[m[K149.txt

W-Agora 4.1.6 - 'modules.php?File' Traversal Arbitrary File Access
| php/webapps/[01;31m[K22[m[K150.txt

W3infotech - Authentication Bypass
| php/webapps/10[01;31m[K22[m[K2.txt

W3Mail 1.0.6 - File Disclosure
| cgi/webapps/[01;31m[K22[m[K015.txt

WarFTPd 1.82.00-RC12 - 'LIST' Format String Denial of Service
| windows/dos/96[01;31m[K22[m[K.py

Web Chat Manager 2.0 - HTML Code Injection
| php/webapps/[01;31m[K22[m[K421.txt

Web Companion versions 5.1.1035.1047 - 'WCAssistantService' Unquoted
Service Path |
windows/local/475[01;31m[K22[m[K.txt

Web Protector 2.0 - Trivial Encryption
| multiple/remote/[01;31m[K22[m[K5[01;31m[K22[m[K.pl

Web Server Creator Web Portal 0.1 - Remote File Inclusion
| php/webapps/[01;31m[K22[m[K044.txt

Web Wiz Forum 6.34 - Information Disclosure
| asp/webapps/[01;31m[K22[m[K507.txt

Web Wiz Site News 3.6 - Information Disclosure
| asp/webapps/[01;31m[K22[m[K487.txt

Web3news 0.95 - 'PHPSECURITYADMIN_PATH' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K69.txt

WebAdmin - Arbitrary File Upload
| php/webapps/1[01;31m[K22[m[K67.txt

WebBBS Pro 1.18 - GET Denial of Service
| windows/dos/[01;31m[K22[m[K759.txt

WebCalendar 0.9.x - Local File Inclusion Information Disclosure
| php/webapps/[01;31m[K22[m[K942.txt

Webchat 0.77 - 'Defines.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K318.txt

WebChat 2.0 - 'users.php' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K716.txt

WebChat 2.0 - 'users.php?Database Username Disclosure
| php/webapps/[01;31m[K22[m[K715.txt

```
Webchat 2.0 Module - Full Path Disclosure
| php/webapps/[01;31m[K22[m[K704.txt

WebCortex WebStores2000 - SQL Injection
| asp/webapps/[01;31m[K22[m[K698.pl

webdesproxy 0.0.1 - 'exec-shield' GET Remote Code Execution
| linux/remote/39[01;31m[K22[m[K.c

Webdrivers Simple Forum - 'message_details.php' SQL Injection
| php/webapps/27[01;31m[K22[m[K.pl

Webfroot Shoutbox 2.32 - 'Expanded.php' Directory Traversal
| php/webapps/[01;31m[K22[m[K705.txt

Webfroot Shoutbox 2.32 - 'Expanded.php' Remote Command Execution
| php/webapps/[01;31m[K22[m[K702.pl

Webfroot Shoutbox 2.32 - 'URI' File Disclosure
| php/webapps/[01;31m[K22[m[K671.txt

Webfroot Shoutbox 2.32 - Remote Command Execution
| php/webapps/[01;31m[K22[m[K687.pl

Webfwlog 0.92 - 'debug.php' Remote File Disclosure
| php/webapps/3[01;31m[K22[m[K2.txt

WeBid 1.0.5 - Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K828.txt

weBid 1.0.5 - Directory Traversal
| php/webapps/[01;31m[K22[m[K829.txt

WebJeff FileManager 1.6 - File Disclosure
| php/webapps/[01;31m[K22[m[K812.txt

WebKitGTK 2.23.90 / WebKitGTK+ 2.[01;31m[K22[m[K.6 - Denial of Service
| linux/dos/46465.txt

WebMethods Integration Server 10.15.0.0000-0092 - Improper Access on
Login Page                              |
windows/remote/5[01;31m[K22[m[K37.txt

Webmin 0.9x / Usermin 0.9x/1.0 - Access Session ID Spoofing
| linux/remote/[01;31m[K22[m[K275.pl

Webmin < 1.290 / Usermin < 1.[01;31m[K22[m[K0 - Arbitrary File
Disclosure                                                  |
multiple/remote/1997.php

Webmin < 1.290 / Usermin < 1.[01;31m[K22[m[K0 - Arbitrary File
Disclosure                                                  |
multiple/remote/2017.pl
```

WebNMS Framework Server 5.2/5.2 SP1 - Multiple Vulnerabilities
| jsp/webapps/40[01;31m[K22[m[K9.txt

WeBProdZ CMS - SQL Injection
| php/webapps/125[01;31m[K22[m[K.txt

WebRTC - FEC Processing Overflow
| multiple/dos/451[01;31m[K22[m[K.txt

Websense Proxy - Filter Bypass
| multiple/dos/[01;31m[K22[m[K935.txt

webSPELL 4.2.0e - 'page' Blind SQL Injection
| php/webapps/86[01;31m[K22[m[K.pl

WebStudio eCatalogue - Blind SQL Injection
| php/webapps/7[01;31m[K22[m[K3.txt

WebStudio eHotel - Blind SQL Injection
| php/webapps/7[01;31m[K22[m[K2.txt

WebSVN 2.0 - Cross-Site Scripting / File Handling / Code Execution
| php/webapps/68[01;31m[K22[m[K.txt

Webyapar 2.0 - Multiple SQL Injections
| php/webapps/4[01;31m[K22[m[K4.txt

Western Digital My Cloud 04.01.03-421/04.01.04-4[01;31m[K22[m[K -
Command Injection |
hardware/webapps/38350.txt

WFChat 1.0 - Information Disclosure
| multiple/remote/[01;31m[K22[m[K388.txt

WhatsUp Gold 20[01;31m[K22[m[K ([01;31m[K22[m[K.1.0 Build 39) - XSS
| multiple/webapps/51781.txt

Wickr Desktop 2.2.1 Windows - Denial of Service
| windows/dos/356[01;31m[K22[m[K.txt

WihPhoto 0.86 dev - 'sendphoto.php' File Disclosure
| php/webapps/[01;31m[K22[m[K282.txt

Wikepage Opus 10 < 2006.2a (lng) - Remote Command Execution
| php/webapps/[01;31m[K22[m[K52.pl

Winamp 5.12 - '.pls' Remote Buffer Overflow (Perl) (2)
| windows/remote/34[01;31m[K22[m[K.pl

Winamp 5.572 - 'whatsnew.txt' (SEH) (Metasploit)
| windows/local/1[01;31m[K22[m[K55.rb

```
WinAsm Studio 5.1.5.0 - Local Heap Overflow (PoC)
| windows/dos/8[01;31m[K22[m[K4.pl

Windows 11 10.0.[01;31m[K22[m[K000 -  Backup service Privilege
Escalation                                                  |
windows/local/51203.txt

Windows 11 [01;31m[K22[m[Kh2 - Kernel Privilege Elevation
| windows/local/51544.c

WinMail Server 4.4 build 1124 - 'WebMail' Remote Add Super User
| php/webapps/36[01;31m[K22[m[K.php

WINMOD 1.4 - '.lst' Local Buffer Overflow (SEH)
| windows/local/9[01;31m[K22[m[K1.pl

WINMOD 1.4 - '.lst' Universal Buffer Overflow (SEH) (2)
| windows/local/9[01;31m[K22[m[K9.py

WinRAR 2.90/3.0/3.10 - Archive File Extension Buffer Overrun
| windows/local/[01;31m[K22[m[K193.txt

WinRAR version 6.[01;31m[K22[m[K - Remote Code Execution via ZIP
archive                                                     |
windows/remote/51935.c

WinRM - VBS Remote Code Execution (Metasploit)
| windows/remote/[01;31m[K22[m[K526.rb

WinUAE 1.4.4 - 'zfile.c' Stack Buffer Overflow
| multiple/dos/309[01;31m[K22[m[K.c

Wireshark 1.0.x - '.ncf' Packet Capture Local Denial of Service
| multiple/dos/66[01;31m[K22[m[K.txt

Wireshark 1.2.1 - GSM A RR Dissector packet.c Remote Denial of Service
| linux/dos/33[01;31m[K22[m[K4.txt

Wireshark 1.2.1 - OpcUa Dissector Resource Exhaustion (Denial of
Service)                                    |
linux/dos/33[01;31m[K22[m[K2.txt

Wireshark 1.2.1 - TLS Dissector 1.2 Conversation Handling Remote Denial
of Service                          | linux/dos/33[01;31m[K22[m[K3.txt

Witango Server 5.0.1.061 - Remote Cookie Buffer Overflow
| multiple/dos/[01;31m[K22[m[K926.txt

Wizz Forum 1.20 - 'TopicID' SQL Injection
| php/webapps/13[01;31m[K22[m[K.pl
```

```
Woltlab Burning Board 1.1.1/2.x - 'galerie_index.php?Username' Cross-
Site Scripting                          |
php/webapps/273[01;31m[K22[m[K.txt

Woltlab Burning Board 2.x - Multiple SQL Injections
| php/webapps/280[01;31m[K22[m[K.txt

WonderCMS 2.1.0 - Cross-Site Request Forgery
| php/webapps/4[01;31m[K22[m[K05.html

WonderCMS 3.4.2 - Remote Code Execution (RCE)
| php/remote/5[01;31m[K22[m[K71.py

Wondershare Filmora 12.2.9.[01;31m[K22[m[K33 - Unquoted Service Path
| windows/local/51395.txt

WooCommerce Customers Manager 29.4 - Post-Authenticated SQL Injection
| multiple/webapps/5[01;31m[K22[m[K48.txt

Wordit Logbook 098b3 - Logbook.pl Remote Command Execution
| cgi/webapps/[01;31m[K22[m[K337.txt

WordPress Core 1.x/2.0.x - Pingback SourceURI Denial of Service /
Information Disclosure                  |
php/webapps/295[01;31m[K22[m[K.py

WordPress Core 2.0 - Comment Post HTML Injection
| php/webapps/27[01;31m[K22[m[K7.txt

WordPress Core 4.7.0/4.7.1 - Content Injection
| linux/webapps/41[01;31m[K22[m[K3.py

WordPress Core 4.7.0/4.7.1 - Content Injection (Ruby)
| linux/webapps/41[01;31m[K22[m[K4.rb

WordPress Core 6.2 - Directory Traversal
| php/webapps/5[01;31m[K22[m[K74.py

WordPress Depicter Plugin 3.6.1 - SQL Injection
| multiple/webapps/5[01;31m[K22[m[K85.py

WordPress Frontend Login and Registration Blocks Plugin 1.0.7 -
Privilege Escalation                    |
multiple/webapps/5[01;31m[K22[m[K91.py

WordPress Plugin Add From Server < 3.3.2 - Cross-Site Request Forgery
(Arbitrary File Upload)                 |
php/webapps/40[01;31m[K22[m[K0.txt

WordPress Plugin Ajax Pagination 1.1 - Local File Inclusion
| php/webapps/326[01;31m[K22[m[K.txt
```

WordPress Plugin All Video Gallery 1.1 - SQL Injection
| php/webapps/[01;31m[K22[m[K427.txt

WordPress Plugin bbPress - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K396.txt

WordPress Plugin Chained Quiz 1.0.8 - 'answer' SQL Injection
| php/webapps/45[01;31m[K22[m[K1.txt

WordPress Plugin chenpress - Arbitrary File Upload
| php/webapps/375[01;31m[K22[m[K.txt

WordPress Plugin Comment Rating 2.9.23 - Multiple Vulnerabilities
| php/webapps/16[01;31m[K22[m[K1.txt

WordPress Plugin Creative Contact Form 0.9.7 - Arbitrary File Upload
| php/webapps/349[01;31m[K22[m[K.txt

WordPress Plugin Download Manager Free 2.7.94 & Pro 4 - (Authenticated)
Persistent Cross-Site Scripting | php/webapps/376[01;31m[K22[m[K.txt

WordPress Plugin Easy Webinar - Blind SQL Injection
| php/webapps/[01;31m[K22[m[K300.txt

WordPress Plugin Facebook Survey 1.0 - SQL Injection
| php/webapps/[01;31m[K22[m[K853.txt

WordPress Plugin FireStorm Professional Real Estate 2.06.01 - SQL
Injection |
php/webapps/[01;31m[K22[m[K071.txt

WordPress Plugin fMoblog 2.1 - 'id' SQL Injection
| php/webapps/8[01;31m[K22[m[K9.txt

WordPress Plugin foxypress 0.4.2.5 - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K374.txt

WordPress Plugin Job Manager 0.7.[01;31m[K22[m[K - Persistent Cross-
Site Scripting |
php/webapps/37738.txt

WordPress Plugin Mail Masta 1.0 - Local File Inclusion (2)
| php/webapps/50[01;31m[K22[m[K6.py

WordPress Plugin Membership Simplified 1.58 - Arbitrary File Download
| php/webapps/416[01;31m[K22[m[K.py

WordPress Plugin Plainview Activity Monitor 20161[01;31m[K22[m[K8 -
(Authenticated) Command Injection |
php/webapps/45274.html

WordPress Plugin Plainview Activity Monitor 20161[01;31m[K22[m[K8 - Remote Code Execution (RCE) (Authenticated) (2) | php/webapps/50110.py

WordPress Plugin Polls 1.2.4 - SQL Injection (PoC)
| php/remote/44[01;31m[K22[m[K9.txt

WordPress Plugin Recipes Blog - 'id' SQL Injection
| php/webapps/31[01;31m[K22[m[K8.txt

WordPress Plugin Ripe HD FLV Player - SQL Injection
| php/webapps/24[01;31m[K22[m[K9.txt

WordPress Plugin social discussions 6.1.1 - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K158.txt

WordPress Plugin Spider Catalog 1.1 - HTML Code Injection / Cross-Site Scripting | php/webapps/[01;31m[K22[m[K463.txt

WordPress Plugin Tagregator 0.6 - Cross-Site Scripting
| php/webapps/45[01;31m[K22[m[K5.txt

WordPress Plugin TinyMCE Thumbnail Gallery 1.0.7 - Remote File Disclosure | php/webapps/190[01;31m[K22[m[K.txt

WordPress Plugin Ultimate Product Catalogue 4.2.2 - SQL Injection
| php/webapps/4[01;31m[K22[m[K63.txt

WordPress Plugin WatuPRO 5.5.1 - SQL Injection
| php/webapps/4[01;31m[K22[m[K91.txt

WordPress Plugin White Label CMS 1.5 - Cross-Site Request Forgery / Persistent Cross-Site Scripting | php/webapps/[01;31m[K22[m[K156.txt

WordPress Plugin Wow Forms 2.1 - SQL Injection
| php/webapps/419[01;31m[K22[m[K.txt

WordPress Plugin WP Symposium 15.1 - Blind SQL Injection
| php/webapps/378[01;31m[K22[m[K.txt

WordPress Plugin WP User Frontend < 2.3.11 - Unrestricted Arbitrary File Upload | php/webapps/394[01;31m[K22[m[K.py

WordPress Plugin WP-Cumulus 1.20 - Full Path Disclosure / Cross-Site Scripting | php/webapps/10[01;31m[K22[m[K8.txt

WordPress Theme Dailyedition-mouss - 'id' SQL Injection
| php/webapps/380[01;31m[K22[m[K.txt

Working Resources 1.7.x/2.15 BadBlue - 'ext.dll' Command Execution
| windows/remote/[01;31m[K22[m[K511.txt

Working Resources BadBlue 1.7.1 - Search Page Cross-Site Scripting
| cgi/webapps/[01;31m[K22[m[K045.txt

Working Resources BadBlue 1.7.x/2.x - Unauthorized HTS Access
| windows/remote/[01;31m[K22[m[K620.txt

Worldweaver DX Studio Player < 3.0.29.1 Firefox plugin - Command Injection |
windows/remote/89[01;31m[K22[m[K.txt

WP All Import v3.6.7 - Remote Code Execution (RCE) (Authenticated)
| php/webapps/511[01;31m[K22[m[K.py

WP-file-manager v6.9 - Unauthenticated Arbitrary File Upload leading to RCE | php/webapps/51[01;31m[K22[m[K4.py

WS Interactive Automne 4.0 - '[01;31m[K22[m[K8-recherche.php' Cross-Site Scripting |
php/webapps/34317.txt

WSMP3 0.0.1/0.0.2 - Multiple Buffer Overflow Vulnerabilities
| linux/dos/[01;31m[K22[m[K033.txt

WSMP3 0.0.1/0.0.2 - Remote Heap Corruption (1)
| linux/remote/[01;31m[K22[m[K034.pl

WSMP3 0.0.1/0.0.2 - Remote Heap Corruption (2)
| linux/remote/[01;31m[K22[m[K035.c

WSMP3 0.0.x - Remote Command Execution
| linux/remote/[01;31m[K22[m[K623.txt

WSMP3 0.0.x - Remote Information Disclosure
| linux/remote/[01;31m[K22[m[K6[01;31m[K22[m[K.txt

WSN Links 2.[01;31m[K22[m[K/2.23 - 'vote.php' SQL Injection
| php/webapps/6524.txt

WTcom 0.2.4-alpha - 'torrents.php' SQL Injection
| php/webapps/[01;31m[K22[m[K00.txt

WU-FTPD 2.6.0/2.6.1/2.6.2 - 'realpath()' Off-by-One Buffer Overflow
| unix/remote/[01;31m[K22[m[K975.c

WU-FTPD 2.6.2 - 'realpath()' Off-by-One Buffer Overflow
| unix/remote/[01;31m[K22[m[K974.c

Xaos 3.0 - Language Option Local Buffer Overflow
| linux/local/[01;31m[K22[m[K748.c

XATABoost 1.0.0 - SQL Injection
| php/webapps/446[01;31m[K22[m[K.txt

Xavi X7028r DSL Router - UPNP Long Request Denial of Service
| hardware/dos/[01;31m[K22[m[K950.txt

XBlast 2.6.1 - 'HOME Environment' Local Buffer Overflow
| linux/local/[01;31m[K22[m[K965.c

Xeneo Web Server 2.2.10 - Undisclosed Buffer Overflow (PoC)
| linux/dos/[01;31m[K22[m[K527.c

Xeneo Web Server 2.2.9 - Denial of Service
| windows/dos/[01;31m[K22[m[K516.pl

Xerver 4.32 - Source Disclosure / HTTP Authentication Bypass
(Metasploit) |
windows/remote/145[01;31m[K22[m[K.rb

XFree86 4.2 - 'XLOCALEDIR' Local Buffer Overflow (1)
| linux/local/[01;31m[K22[m[K320.c

XFree86 4.2 - 'XLOCALEDIR' Local Buffer Overflow (2)
| linux/local/[01;31m[K22[m[K321.c

XFree86 4.2 - 'XLOCALEDIR' Local Buffer Overflow (3)
| linux/local/[01;31m[K22[m[K3[01;31m[K22[m[K.c

XFree86 4.2 - 'XLOCALEDIR' Local Buffer Overflow (4)
| linux/local/[01;31m[K22[m[K323.c

XFree86 X11R6 3.3.x - Font Server Remote Buffer Overrun
| unix/remote/[01;31m[K22[m[K036.pl

xfstt 1.2/1.4 - Memory Disclosure
| linux/dos/[01;31m[K22[m[K952.txt

Ximian Evolution 1.x - MIME image/* Content-Type Data Inclusion
| linux/remote/[01;31m[K22[m[K371.txt

Ximian Evolution 1.x - UUEncoding Denial of Service
| linux/dos/[01;31m[K22[m[K370.txt

Ximian Evolution 1.x - UUEncoding Parsing Memory Corruption
| linux/remote/[01;31m[K22[m[K369.txt

Xinetd 2.1.x/2.3.x - Rejected Connection Memory Leakage Denial of
Service |
linux/dos/[01;31m[K22[m[K508.sh

Xivo 1.2 - Arbitrary File Download
| php/webapps/[01;31m[K22[m[K548.txt

Xlink FTP Client - Remote Buffer Overflow (Metasploit)
| windows/remote/167[01;31m[K22[m[K.rb

XM Easy Personal FTP Server 5.8.0 - Remote Denial of Service
| windows/dos/10[01;31m[K22[m[K1.txt

Xmail 0.5/0.6 CTRLServer - Arbitrary Commands
| linux/remote/206[01;31m[K22[m[K.c

XMame 0.6x - Lang Local Buffer Overflow
| linux/local/[01;31m[K22[m[K703.c

XMB Forum 1.8 - 'buddy.php?action' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K821.txt

XMB Forum 1.8 - 'member.php' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K632.txt

XMB Forum 1.8 - 'member.php' SQL Injection
| php/webapps/[01;31m[K22[m[K521.c

XMB Forum 1.8 - 'member.php?member' Cross-Site Scripting
| php/webapps/[01;31m[K22[m[K820.txt

Xonic.ru News 1.0 - 'script.php' Remote Command Execution
| php/webapps/[01;31m[K22[m[K501.txt

Xoops 1.3.5 - Private Message System Font Attributes HTML Injection
| php/webapps/[01;31m[K22[m[K080.txt

Xoops 1.3.x/2.0 MyTextSanitizer - HTML Injection
| php/webapps/[01;31m[K22[m[K539.txt

XOOPS 2.0 XoopsOption - Information Disclosure
| php/webapps/[01;31m[K22[m[K389.txt

XOOPS Module icontent 1.0/4.5 - Remote File Inclusion
| php/webapps/40[01;31m[K22[m[K.html

xorg-x11-server < 1.20.3 - 'modulepath' Local Privilege Escalation
| multiple/local/459[01;31m[K22[m[K.sh

XPCD 2.0.8 - 'HOME Environment' Local Buffer Overflow
| linux/local/[01;31m[K22[m[K996.c

Xpressions Interactive - Multiple SQL Injections
| asp/webapps/[01;31m[K22[m[K724.txt

XRms 1.99.2 - 'last_name' Cross-Site Scripting
| php/webapps/323[01;31m[K22[m[K.txt

xsoldier 0.96 (RedHat 6.2) - Local Buffer Overflow
| linux/local/[01;31m[K22[m[K9.c

```
Xt Library - Local Privilege Escalation
| linux/local/3[01;31m[K22[m[K.c

Xtokkaetama 1.0 b-6 - Nickname Local Buffer Overflow (1)
| linux/local/[01;31m[K22[m[K984.c

Xtokkaetama 1.0 b-6 - Nickname Local Buffer Overflow (2)
| linux/local/[01;31m[K22[m[K985.c

Xynph FTP Server 1.0 - Directory Traversal
| windows/remote/[01;31m[K22[m[K144.txt

YaBB 1 Gold SP 1 - 'YaBB.pl' Cross-Site Scripting
| cgi/webapps/[01;31m[K22[m[K052.txt

YABB 1.4.1 SE - 'Reminder.php' SQL Injection
| php/webapps/[01;31m[K22[m[K146.txt

YABB SE 0.8/1.4/1.5 - 'Packages.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K192.pl

YACS CMS 6.6.1 - context[path_to_root] Remote File Inclusion
| php/webapps/[01;31m[K22[m[K82.txt

Yahoo! Messenger - 'YVerInfo.dll' ActiveX Control Buffer Overflow
(Metasploit)                                |
windows/remote/165[01;31m[K22[m[K.rb

Yahoo! Voice Chat ActiveX Control 1.0.0.43 - Remote Buffer Overflow
| windows/remote/[01;31m[K22[m[K593.html

Yandex.Server 2010 9.0 - 'text' Cross-Site Scripting
| php/webapps/37[01;31m[K22[m[K4.txt

YapBB 1.2 - 'class_yapbbcooker.php' Remote File Inclusion
| php/webapps/3[01;31m[K22[m[K44.txt

Yappa-ng 2.3.1 - 'admin_modules' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K92.txt

Yellow Swordfish Simple Forum 1.x - 'sf-profile.php' SQL Injection
| php/webapps/31[01;31m[K22[m[K7.txt

Yelp 2.23.1 - Invalid URI Format String
| linux/dos/3[01;31m[K22[m[K48.txt

Yii Framework 1.1.8 - Search SQL Injection
| php/webapps/[01;31m[K22[m[K877.txt

Yogurt Social Network 3.2 rc1 Module for XOOPS - 'album.php?uid' Cross-
Site Scripting                        |
php/webapps/3[01;31m[K22[m[K00.txt
```

```
Yogurt Social Network 3.2 rc1 Module for XOOPS - 'index.php?uid' Cross-
Site Scripting                      |
php/webapps/3[01;31m[K22[m[K02.txt

Yogurt Social Network 3.2 rc1 Module for XOOPS - 'scrapbook.php?uid'
Cross-Site Scripting                 |
php/webapps/3[01;31m[K22[m[K01.txt

Yogurt Social Network 3.2 rc1 Module for XOOPS - 'tribes.php?uid'
Cross-Site Scripting                    |
php/webapps/3[01;31m[K22[m[K03.txt

Yokogawa CENTUM CS 3000 - 'BKBCopyD.exe' Remote Buffer Overflow
(Metasploit)                              |
windows/remote/3[01;31m[K22[m[K10.rb

Yokogawa CENTUM CS 3000 - 'BKHOdeq.exe' Remote Buffer Overflow
(Metasploit)                               |
windows/remote/3[01;31m[K22[m[K09.rb

Youbin 2.5/3.0/3.4 - 'HOME' Buffer Overflow
| freebsd/local/[01;31m[K22[m[K566.pl

Youngzsoft CMailServer 4.0 - 'RCPT TO' Buffer Overflow
| windows/dos/[01;31m[K22[m[K582.pl

Youngzsoft CMailServer 4.0 - MAIL FROM Buffer Overflow
| windows/dos/[01;31m[K22[m[K581.pl

YourFreeWorld Ad-Exchange Script - 'id' SQL Injection
| php/webapps/3[01;31m[K22[m[K80.txt

yPlay 1.0.76 - '.mp3' Local Crash (PoC)
| windows/dos/11[01;31m[K22[m[K7.pl

YUI Images Script - Arbitrary File Upload
| php/webapps/1[01;31m[K22[m[K27.txt

YzmCMS 5.3 - 'Host' Header Injection
| php/webapps/474[01;31m[K22[m[K.txt

Zabbix 7.0.0 - SQL Injection
| php/webapps/5[01;31m[K22[m[K30.py

ZAPms 1.[01;31m[K22[m[K - 'nick' SQL Injection
| php/webapps/35734.txt

Zblast 1.2 - 'Username' Local Buffer Overrun
| linux/local/[01;31m[K22[m[K745.c

ZenPhoto 1.4.3.3 - Multiple Vulnerabilities
| php/webapps/[01;31m[K22[m[K524.txt
```

```
Zentrack 2.2/2.3/2.4 - 'index.php' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K750.txt

ZeroBoardXE 1.1.5 (09.01.[01;31m[K22[m[K) - Cross-Site Scripting
| php/webapps/8019.txt

Zeroo HTTP Server 1.5 - Directory Traversal (1)
| linux/remote/[01;31m[K22[m[K063.c

Zeroo HTTP Server 1.5 - Directory Traversal (2)
| linux/remote/[01;31m[K22[m[K064.pl

Zervit Web Server 0.3 - sockets++ crash Remote Denial of Service
| windows/dos/85[01;31m[K22[m[K.pl

Zeus Web Server 4.0/4.1 - Admin Interface Cross-Site Scripting
| cgi/remote/[01;31m[K22[m[K000.txt

Zeus Web Server 4.x - Admin Interface 'VS_Diag.cgi' Cross-Site
Scripting                                    |
cgi/webapps/[01;31m[K22[m[K692.txt

ZeusCart - 'prodid' SQL Injection
| php/webapps/39[01;31m[K22[m[K3.txt

ZeusCart 4.0 - Cross-Site Request Forgery
| php/webapps/38[01;31m[K22[m[K3.txt

ZeusCart 4.0 - SQL Injection
| php/webapps/38[01;31m[K22[m[K4.txt

zFTP Client 20061[01;31m[K22[m[K0 - 'Connection Name' Local Buffer
Overflow                                                |
linux/local/40203.py

ZipCentral 4.01 - '.ZIP' File Handling Local Buffer Overflow
| windows/local/[01;31m[K22[m[K78.cpp

zkfingerd 0.9.1 - 'say()' Format String
| linux/remote/[01;31m[K22[m[K101.c

zkfingerd SysLog 0.9.1 - Format String
| linux/remote/[01;31m[K22[m[K091.c

ZKSoftware Biometric Attendence Managnmnet Hardware[MIPS] 2 - Improper
Authentication                        |
hardware/remote/118[01;31m[K22[m[K.txt

ZKTeco ZKTime.Net 3.0.1.6 - Insecure File Permissions Privilege
Escalation                                    |
windows/local/403[01;31m[K22[m[K.txt
```

```
zKup CMS 2.0 < 2.3 - Arbitrary File Upload
| php/webapps/5[01;31m[K22[m[K0.php

Zlib 1.1.4 - Compression Library 'gzprintf()' Buffer Overrun (1)
| linux/dos/[01;31m[K22[m[K273.c

Zlib 1.1.4 - Compression Library 'gzprintf()' Buffer Overrun (2)
| linux/remote/[01;31m[K22[m[K274.c

ZoIPer 2.[01;31m[K22[m[K - Call-Info Remote Denial of Service
| multiple/dos/9987.py

Zoner Photo Studio 15 b3 - Buffer Overflow (PoC)
| windows/dos/[01;31m[K22[m[K685.txt

Zoner Photo Studio 15 Build 3 - 'Zps.exe' Registry Value Parsing
| windows/local/[01;31m[K22[m[K652.py

Zookeeper 3.5.2 Client - Denial of Service
| multiple/dos/4[01;31m[K22[m[K94.py

Zortam MP3 Media Studio 23.95 - Denial of Service (PoC)
| windows_x86-64/dos/45[01;31m[K22[m[K2.py

ZPanel 10.0.1 - Cross-Site Request Forgery / Cross-Site Scripting / SQL
Injection / Password Reset         |
multiple/webapps/[01;31m[K22[m[K490.txt

ZTE - Change Admin Password
| cgi/webapps/187[01;31m[K22[m[K.txt

ZTE ZXV10 H201L - RCE via authentication bypass
| multiple/local/5[01;31m[K22[m[K79.py

Zyke CMS 1.1 - Authentication Bypass
| php/webapps/1[01;31m[K22[m[K62.php

ZYXEL P-660HN-T1A Router - Authentication Bypass
| hardware/webapps/3[01;31m[K22[m[K04.txt

Zyxel USG FLEX H series uOS 1.31 - Privilege Escalation
| multiple/local/5[01;31m[K22[m[K93.bash

ZZ:FlashChat 3.1 - 'adminlog' Remote File Inclusion
| php/webapps/[01;31m[K22[m[K24.txt
```

```
---------------------------------------------------------------------------------------- ----------
----------

---------------------------------------------------------------------------------------- ----------
----------
Shellcode Title
|  Path

---------------------------------------------------------------------------------------- ----------
----------
BSD/x86 - Bind ([01;31m[K22[m[K[01;31m[K22[m[K/TCP) Shell Shellcode
(100 bytes)                                                                 |
bsd_x86/43629.c

BSD/x86 - Reverse
(torootteam.host.sk:[01;31m[K22[m[K[01;31m[K22[m[K/TCP) Shell Shellcode
(93 bytes)                                  | bsd_x86/13254.c

BSD/x86 - setuid(0) + Break chroot (../ 10x Loop) + Bind
([01;31m[K22[m[K[01;31m[K22[m[K/TCP) Shell Shellcode (133 bytes)
| bsd_x86/43628.c

FreeBSD/x86 - Bind (4883/TCP) Shell (/bin/sh) + Password Shellcode
([01;31m[K22[m[K2 bytes)                                |
freebsd_x86/13270.c

Linux - Reverse (/TCP) Shell + Multi/Dual Mode Shellcode (129 bytes)
(Generator)                             | generator/41[01;31m[K22[m[K0.c

Linux/ARM - chmod(/etc/shadow 0777) Shellcode (35 bytes)
| arm/141[01;31m[K22[m[K.c

Linux/MIPS - reboot() Shellcode (32 bytes)
| linux_mips/18[01;31m[K22[m[K7.c

Linux/MIPS - Reverse (0x7a69/TCP) Shell Shellcode (168 bytes)
| linux_mips/18[01;31m[K22[m[K6.c

Linux/x64 - Bind (4442/TCP) Shell + Syscall Persistent + Multi-
Terminal/Port-Range (4444-4447/TCP) + Passw | linux_x86-
64/401[01;31m[K22[m[K.c

Linux/x64 - execve() Shellcode ([01;31m[K22[m[K bytes)
| linux_x86-64/38239.asm

Linux/x64 - execve(/bin/sh) Shellcode ([01;31m[K22[m[K bytes)
| linux_x86-64/41174.nasm

Linux/x64 - Kill All Processes Shellcode (19 bytes)
| linux_x86-64/425[01;31m[K22[m[K.c
```

Linux/x64 - Reverse (10.1.1.4:46357/TCP) Shell + Subtle Probing + Timer + Burst + Password (la crips) + Mu | linux_x86-64/40139.c

Linux/x64 - Reverse (127.0.0.1:4444/TCP) Shell (/bin/sh) + Password (hack) + Polymorphic Shellcode (1[01;31m[K22[m[K by | linux_x86-64/39383.c

Linux/x86 - Bind (4444/TCP) Shell (/bin/sh) + Null-Free Shellcode (75 bytes) | linux_x86/4[01;31m[K22[m[K54.c

Linux/x86 - Bind (5074/TCP) Shell + ToUpper Encoded Shellcode ([01;31m[K22[m[K6 bytes) | linux_x86/13427.c

Linux/x86 - Bind (8000/TCP) Shell + Add Root User Shellcode ([01;31m[K22[m[K5+ bytes) | linux_x86/13318.s

Linux/x86 - Bind (9090/TCP) Shell (/bin/zsh) Shellcode (96 bytes) | linux_x86/40[01;31m[K22[m[K2.c

Linux/x86 - Download File (http://192.168.2.[01;31m[K22[m[K2/x) + chmod() + Execute Shellcode (108 bytes) | linux_x86/43748.c

Linux/x86 - Egg Omelet (Multi-Egghunter) + Reverse (192.168.1[01;31m[K22[m[K.1:43981/TCP) Shell (/bin/sh) Shellcode | linux_x86/28474.c

Linux/x86 - execve() Shellcode (23 bytes) | linux_x86/134[01;31m[K22[m[K.c

Linux/x86 - execve(/bin/sh) Shellcode ([01;31m[K22[m[K bytes) | linux_x86/13354.c

Linux/x86 - execve(/bin/sh) Shellcode (23 bytes) (2) | linux_x86/437[01;31m[K22[m[K.c

Linux/x86 - File Unlinker Shellcode (18+ bytes) | linux_x86/133[01;31m[K22[m[K.c

Linux/x86 - Remote Port Forwarding (ssh -R 9999:localhost:[01;31m[K22[m[K 192.168.0.[01;31m[K22[m[K6) Shellcode (87 bytes) | linux_x86/236[01;31m[K22[m[K.c

Linux/x86 - Reverse (127.0.0.1:53/UDP) Shell (/bin/sh) Shellcode (668 bytes) | linux_x86/4[01;31m[K22[m[K08.nasm

Linux/x86 - Reverse (127.1.1.1:11111/TCP) Shell + Null-Free Shellcode (67 bytes) | linux_x86/4[01;31m[K22[m[K95.c

```
Linux/x86 - Reverse (127.255.255.254:9090/TCP) Shell (/bin/zsh)
Shellcode (80 bytes)                        |
linux_x86/40[01;31m[K22[m[K3.c

Linux/x86 - Reverse (192.168.13.[01;31m[K22[m[K:31337/TCP) Shell
(/bin/sh) Shellcode (82 bytes) (Generator)             |
generator/13364.c

Linux/x86 - Reverse (192.168.[01;31m[K22[m[K7.129:4444/TCP) Shell
(/bin/sh) Shellcode (75 bytes)                         |
linux_x86/40075.c

Linux/x86 - Reverse (::ffff:192.168.64.129:1472/TCP) Shell (/bin/sh) +
IPv6 Shellcode (159 bytes)          | linux_x86/397[01;31m[K22[m[K.c

Linux/x86 - Reverse (localhost:8080/TCP) Shell + SSL Shellcode
(4[01;31m[K22[m[K bytes)                                    |
linux_x86/17371.c

Linux/x86 - Reverse TCP Shellcode (95 bytes)
| linux_x86/5[01;31m[K22[m[K97.c

Linux/x86 - setuid(0) + chmod 0666 /etc/shadow + Polymorphic Shellcode
(61 bytes)                          | linux_x86/137[01;31m[K22[m[K.c

Linux/x86 - Socket-Proxy (31337:11.[01;31m[K22[m[K.33.44:80) Shellcode
(372 bytes)                                       | linux_x86/13402.c

Linux/x86-64 - execve(_/bin/sh_) Shellcode (36 bytes)
| linux_x86-64/5[01;31m[K22[m[K96.asm

Linux/x86_64 - execve(/bin/sh) Shellcode ([01;31m[K22[m[K bytes)
| linux_x86-64/47008.c

OSX/PPC - Add inetd (/etc/inetd.conf) Backdoor (Bind 6969/TCP Shell)
Shellcode ([01;31m[K22[m[K2 bytes)                | osx_ppc/13482.c

OSX/PPC - Create /tmp/suid Shellcode (1[01;31m[K22[m[K bytes)
| osx_ppc/13485.c

OSX/x64 - Reverse (FFFFFFFF:4444/TCP) Shell (/bin/sh) Shellcode (131
bytes)                                | osx/17[01;31m[K22[m[K4.s

Safari 4.0.5 < 5.0.0 (Windows XP/7) - JavaScript JITed exec calc
(ASLR/DEP Bypass) + Null-Free Shellcode   |
windows/14[01;31m[K22[m[K1.html

Solaris/SPARC - Bind (2001/TCP) Shell (/bin/sh) Shellcode
| solaris_sparc/436[01;31m[K22[m[K.asm

Solaris/SPARC - Bind (6789/TCP) Shell (/bin/sh) Shellcode
([01;31m[K22[m[K8 bytes)                                      |
solaris_sparc/13495.c
```

Windows (XP Professional SP3) - calc.exe (C:/WINDOWS/system32/calc.exe)
ROP Shellcode (428 bytes) | windows/[01;31m[K22[m[K489.cpp

Windows 11 x64 - Reverse TCP Shellcode (564 bytes)
| windows_x86-64/5[01;31m[K22[m[K98.py

Windows/x64 - Dynamic MessageBoxA or MessageBoxW PEB & Import Table
Method Shellcode (232 bytes) | windows_x86-
64/48[01;31m[K22[m[K9.txt

Windows/x86 - Download File (http://www.ph4nt0m.org/a.exe) + Execute
(C:/a.exe) Shellcode ([01;31m[K22[m[K6+ bytes) |
windows_x86/135[01;31m[K22[m[K.c

Windows/x86 - Locate kernel32 base address / Stack Crack method
NullFree Shellcode (171 bytes) |
windows_x86/507[01;31m[K22[m[K.asm

Windows/x86 - SE_DACL_PROTECTED Protect Process Shellcode
([01;31m[K22[m[K9 bytes) |
windows_x86/41381.c

Windows/x86 - system(systeminfo) Shellcode ([01;31m[K22[m[K4 bytes)
| windows_x86/39914.c

Port: 23

Exploit Title
| Path

(SSH.com Communications) SSH Tectia (SSH < 2.0-6.1.9.95 / Tectia
6.1.9.95) - Remote Authentication Bypass |
linux/remote/[01;31m[K23[m[K082.txt

(SSH.com Communications) SSH Tectia - USERAUTH Change Request Password
Reset (Metasploit) | unix/remote/[01;31m[K23[m[K156.rb

0irc-client 1345 build200608[01;31m[K23[m[K - Denial of Service
| windows/dos/3547.c

0verkill 0.16 - Game Client Multiple Local Buffer Overflow
Vulnerabilities |
linux/local/[01;31m[K23[m[K634.c

```
1[01;31m[K23[m[K Flash Chat 5.0 - Remote Code Injection
| php/webapps/27121.txt

1[01;31m[K23[m[K Flash Chat 7.8 - Multiple Vulnerabilities
| php/webapps/34481.txt

1[01;31m[K23[m[K FlashChat 7.8 - Multiple Vulnerabilities
| windows/remote/14658.txt

1[01;31m[K23[m[KtkShop 0.9.1 - Remote Authentication Bypass
| php/webapps/4733.txt

15 TOTOLINK Router Models - Multiple Remote Code Execution
Vulnerabilities                                  |
hardware/webapps/376[01;31m[K23[m[K.txt

1st Class Internet Solutions 1st Class Mail Server 4.0 - Remote Buffer
Overflow (PoC)                       |
multiple/dos/[01;31m[K23[m[K787.txt

1st Class Mail Server 4.0 1 - advanced.tagz Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K941.txt

1st Class Mail Server 4.0 1 - general.tagz Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K940.txt

1st Class Mail Server 4.0 1 - Index Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K938.txt

1st Class Mail Server 4.0 1 - list.tagz Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K942.txt

1st Class Mail Server 4.0 1 - members.tagz Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K939.txt

1st Class Mail Server 4.0 1 - viewmail.tagz Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K937.txt

212Cafe WebBoard 2.90 Beta - Remote File Disclosure
| php/webapps/88[01;31m[K23[m[K.txt

[01;31m[K23[m[K45 Security Guard 3.7 - '[01;31m[K23[m[K45BdPcSafe.sys'
Denial of Service                                          |
windows/dos/44615.cpp

[01;31m[K23[m[K45 Security Guard 3.7 -
'[01;31m[K23[m[K45NetFirewall.sys' Denial of Service
| windows_x86/dos/44600.c

[01;31m[K23[m[K45 Security Guard 3.7 - '[01;31m[K23[m[K45NsProtect.sys'
Denial of Service                                          |
windows/dos/44619.cpp
```

2DayBiz Advanced Poll Script - Cross-Site Scripting / Authentication Bypass |
php/webapps/1[01;31m[K23[m[K95.txt

2Moons 1.4 - Multiple Remote File Inclusions
| php/webapps/362[01;31m[K23[m[K.txt

2WIRE HomePortal Series - Directory Traversal
| windows/remote/[01;31m[K23[m[K562.html

32bit FTP - 'PASV' Reply Client Remote Overflow (Metasploit)
| windows_x86/remote/86[01;31m[K23[m[K.rb

3Com SuperStack 3 Firewall - Content Filter Bypassing
| multiple/remote/2[01;31m[K23[m[K27.txt

@Mail 5.42 and @Mail WebMail 5.0.5 - Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/3[01;31m[K23[m[K17.txt

Aanval 7.1 build 70151 - Multiple Vulnerabilities
| php/webapps/287[01;31m[K23[m[K.txt

Aardvark Topsites 4.1 PHP - Multiple Vulnerabilities
| php/webapps/[01;31m[K23[m[K443.txt

ABB Cylon Aspect 3.08.02 - Cross-Site Request Forgery (CSRF)
| multiple/hardware/52[01;31m[K23[m[K1.html

ABB Cylon Aspect 3.08.03 (webServerDeviceLabelUpdate.php) - File Write DoS |
php/hardware/52[01;31m[K23[m[K4.txt

ABB Cylon Aspect 3.08.03 - Guest2Root Privilege Escalation
| multiple/remote/5[01;31m[K23[m[K05.py

ABB Cylon Aspect 3.08.03 - Hard-coded Secrets
| multiple/webapps/522[01;31m[K23[m[K.txt

ABB Cylon Aspect 3.08.04 DeploySource - Remote Code Execution (RCE)
| multiple/remote/5[01;31m[K23[m[K17.txt

ABB Cylon Aspect 4.00.00 (factorySaved.php) - Unauthenticated XSS
| php/hardware/52[01;31m[K23[m[K3.txt

ABB Cylon Aspect 4.00.00 (factorySetSerialNum.php) - Remote Code Execution |
php/hardware/52[01;31m[K23[m[K2.txt

ABB Cylon Aspect Studio 3.08.03 - Binary Planting
| multiple/local/5[01;31m[K23[m[K06.txt

```
aBitWhizzy - 'abitwhizzy.php' Information Disclosure
| php/webapps/28[01;31m[K23[m[K.txt

AbleSpace 1.0 - 'adv_cat.php' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K02.txt

Aborior Encore Web Forum - Arbitrary Command Execution
| cgi/webapps/[01;31m[K23[m[K907.pl

Abyss Web Server 1.0/1.1 - Authentication Bypass
| windows/remote/[01;31m[K23[m[K419.txt

Accellion File Transfer Appliance Error Report Message - Open Email
Relay                                  |
multiple/remote/3[01;31m[K23[m[K82.txt

Accellion Secure File Transfer Appliance - Multiple Command Restriction
/ Privilege Escalations            | linux/local/336[01;31m[K23[m[K.txt

Accipiter DirectServer 6.0 - Remote File Disclosure
| windows/remote/[01;31m[K23[m[K533.txt

ACGV News 0.9.1 - 'article.php' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K07.txt

ACGV News 0.9.1 - 'header.php' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K24.txt

Achievo 1.4.5 - Multiple Vulnerabilities (2)
| php/webapps/[01;31m[K23[m[K253.txt

ACLogic CesarFTP 0.99 - Remote Resource Exhaustion (Denial of Service)
| windows/dos/[01;31m[K23[m[K700.txt

Acme thttpd 1.9/2.0.x - CGI Test Script Cross-Site Scripting
| cgi/remote/[01;31m[K23[m[K582.txt

Acritum Femitter 1.03 - Directory Traversal
| windows/remote/1[01;31m[K23[m[K10.txt

ACS Blog 0.8/0.9/1.0/1.1 - 'search.asp' Cross-Site Scripting
| asp/webapps/25[01;31m[K23[m[K3.txt

ActivePDF Toolkit < 8.1.0.190[01;31m[K23[m[K - Multiple Memory
Corruptions                                                |
windows/dos/44251.txt

ActualAnalyzer Server 8.[01;31m[K23[m[K - 'rf' Remote File Inclusion
| php/webapps/1767.txt

Acuity CMS 2.6.2 - '/admin/file_manager/browse.asp?path' Traversal
Arbitrary File Access                  |
asp/webapps/372[01;31m[K23[m[K.txt
```

```
Acunetix WVS 10.0 Build 201506[01;31m[K23[m[K - Denial of Service (PoC)
| windows/dos/45186.py

Ad Manager Pro 2.6 - 'ipath' Remote File Inclusion
| php/webapps/19[01;31m[K23[m[K.txt

ADA IMGSVR 0.4 - Arbitrary File Download
| windows/remote/[01;31m[K23[m[K906.txt

ada imgsvr 0.4 - Directory Traversal
| windows/remote/[01;31m[K23[m[K909.txt

ADA IMGSVR 0.4 - Remote Directory Listing
| windows/remote/[01;31m[K23[m[K905.txt

AdaptCMS 2.0.1 Beta - Remote File Inclusion (Metasploit)
| php/webapps/15[01;31m[K23[m[K7.rb

Add a link 4 - Security Bypass / SQL Injection
| php/webapps/3[01;31m[K23[m[K92.pl

ADI Convergence Galaxy FTP Server Password - Remote Denial of Service
| windows/dos/313[01;31m[K23[m[K.c

Adobe - 'Doc.media.newPlayer' Use-After-Free (Metasploit) (2)
| windows/local/166[01;31m[K23[m[K.rb

Adobe Acrobat 9.1.2 NOS - Local Privilege Escalation
| windows/local/92[01;31m[K23[m[K.txt

Adobe Flash (Linux x64) - Bad Dereference at 0x[01;31m[K23[m[Kc
| linux_x86-64/dos/37868.txt

Adobe Flash - YUVPlane Decoding Heap Overflow
| multiple/dos/414[01;31m[K23[m[K.txt

Adobe Flash Player - ByteArray Use-After-Free (Metasploit)
| multiple/remote/375[01;31m[K23[m[K.rb

Adobe Flash Player 11.5.502.135 - Crash (PoC)
| windows/dos/[01;31m[K23[m[K469.txt

Adobe Flash Player [01;31m[K23[m[K.0.0.162 - '.SWF' ConstantPool
Critical Memory Corruption                                  |
multiple/dos/40510.txt

Adobe IndesignServer 5.5 - SOAP Server Arbitrary Script Execution
(Metasploit)                                |
multiple/remote/[01;31m[K23[m[K178.rb

Adobe Photoshop 8.0 - COM Objects Denial of Service
| windows/dos/[01;31m[K23[m[K915.txt
```

```
Adobe SVG Viewer 3.0 - 'postURL'/'getURL' Restriction Bypass
| multiple/remote/[01;31m[K23[m[K[01;31m[K23[m[K0.txt

Adult Directory - 'cat_id' SQL Injection
| php/webapps/4[01;31m[K23[m[K8.txt

Advanced Comment System 1.0 - Multiple Remote File Inclusions
| php/webapps/96[01;31m[K23[m[K.txt

Advanced Guestbook 2.4.0 - 'phpBB' File Inclusion
| php/webapps/17[01;31m[K23[m[K.txt

Advanced Image Hosting (AIH) 2.3 - 'gal' Blind SQL Injection
| php/webapps/8[01;31m[K23[m[K8.txt

Advanced Webhost Billing System (AWBS) 2.7.1 - 'news.php' SQL Injection
| php/webapps/58[01;31m[K23[m[K.txt

Advanced Webhost Billing System (AWBS) 2.9.2 - 'oid' SQL Injection
| php/webapps/35[01;31m[K23[m[K1.txt

Advantech Studio 7.0 - SCADA/HMI Directory Traversal
| windows/webapps/[01;31m[K23[m[K132.py

Advantech Webaccess HMI/SCADA Software - Persistence Cross-Site
Scripting                                  |
asp/webapps/[01;31m[K23[m[K968.txt

aeDating 4.1 - dir[inc] Remote File Inclusion
| php/webapps/[01;31m[K23[m[K77.txt

Affiliate Software Java 4.0 - Authentication Bypass
| asp/webapps/74[01;31m[K23[m[K.txt

Agilebio Lab Collector Electronic Lab Notebook  v4.[01;31m[K23[m[K4 -
Remote Code Execution (RCE)                        |
php/webapps/51307.py

Agnitum Outpost Firewall 3.5.631 - 'FiltNT.SYS' Local Denial of Service
| windows/dos/28[01;31m[K23[m[K2.txt

AIOCP 1.3.x - 'cp_dpage.php' SQL Injection
| php/webapps/289[01;31m[K23[m[K.txt

aiptek netcam WebServer 0.93.15 - Directory Traversal
| multiple/remote/[01;31m[K23[m[K557.txt

AirKeyboard iOS App 1.0.5 - Remote Input Injection
| ios/remote/5[01;31m[K23[m[K33.py

AIX 4.3.3/5.1 - Invscoutd Symbolic Link
| aix/local/[01;31m[K23[m[K883.pl
```

AIX 4.3.3/5.x - Getlvcb Command Line Argument Buffer Overflow (1)
| aix/local/[01;31m[K23[m[K840.pl

AIX 4.3.3/5.x - Getlvcb Command Line Argument Buffer Overflow (2)
| aix/local/[01;31m[K23[m[K841.c

AJ Matrix 3.1 - 'id' Multiple SQL Injections
| php/webapps/1[01;31m[K23[m[K46.txt

AJ Shopping Cart 1.0 (maincatid) - SQL Injection
| php/webapps/1[01;31m[K23[m[K49.txt

AjentiCP 1.2.[01;31m[K23[m[K.13 - Cross-Site Scripting
| php/webapps/45691.txt

Akarru 0.4.3.34 - 'bm_content' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K15.txt

Aktiv Player 2.80 - Crash (PoC)
| windows/dos/[01;31m[K23[m[K780.py

Alabanza Control Panel 3.0 - Domain Modification
| cgi/remote/20[01;31m[K23[m[K8.txt

Aladdin Knowledge System Ltd - 'ChooseFilePath' Remote Buffer Overflow
(Metasploit) |
windows/remote/2[01;31m[K23[m[K75.rb

Aladdin Knowledge System Ltd - 'PrivAgent.ocx' ChooseFilePath Buffer
Overflow |
windows/remote/2[01;31m[K23[m[K01.html

Alan Ward A-CART 2.0 - 'category.asp?catcode' SQL Injection (2)
| asp/webapps/[01;31m[K23[m[K891.txt

Alan Ward A-Cart 2.0 - MSG Cross-Site Scripting
| asp/webapps/[01;31m[K23[m[K195.txt

AldWeb MiniPortail 1.9/2.x - 'LNG' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K065.txt

All Enthusiast ReviewPost PHP Pro 2.5 - 'showcat.php' SQL Injection
| php/webapps/[01;31m[K23[m[K646.txt

All Enthusiast ReviewPost PHP Pro 2.5 - 'showproduct.php' SQL Injection
| php/webapps/[01;31m[K23[m[K645.txt

Allegro RomPager 2.10 - URL Request Denial of Service
| hardware/dos/10[01;31m[K23[m[K7.txt

Allied Telesis AT-MCF2000M 3.0.2 - Remote Command Execution
| hardware/remote/[01;31m[K23[m[K855.txt

ALLMediaServer 0.95 - Remote Buffer Overflow
| windows/remote/435[01;31m[K23[m[K.py

AllMyGuests 0.x - 'info.inc.php' Arbitrary Code Execution
| php/webapps/[01;31m[K23[m[K697.txt

AllMyLinks 0.x - 'footer.inc.php' Arbitrary Code Execution
| php/webapps/[01;31m[K23[m[K699.txt

AllMyVisitors 0.x - 'info.inc.php' Arbitrary Code Execution
| php/webapps/[01;31m[K23[m[K698.txt

Alstrasoft AskMe Pro 2.1 - 'que_id' SQL Injection
| php/webapps/1[01;31m[K23[m[K72.txt

Alstrasoft e-Friends 4.85 - Remote Command Execution
| php/webapps/[01;31m[K23[m[K89.pl

Alt-N MDaemon 6.x/WorldClient - Form2Raw Raw Message Handler Buffer
Overflow (1) |
windows/dos/[01;31m[K23[m[K501.c

Alt-N MDaemon 6.x/WorldClient - Form2Raw Raw Message Handler Buffer
Overflow (2) |
windows/remote/[01;31m[K23[m[K502.c

Alt-N MDaemon Server 2.71 SP1 - SMTP HELO Argument Buffer Overflow
| windows/dos/[01;31m[K23[m[K146.c

Alumni 1.0.8/1.0.9 - 'info.php?id' SQL Injection
| php/webapps/317[01;31m[K23[m[K.txt

AMember Pro 2.3.4 - Remote File Inclusion
| php/webapps/26[01;31m[K23[m[K7.txt

AMX Corp. VNC ActiveX Control - 'AmxVnc.dll 1.0.13.0' Remote Buffer
Overflow |
windows/remote/41[01;31m[K23[m[K.html

Anchor CMS 0.12.7 - Stored Cross Site Scripting (XSS)
| php/webapps/5[01;31m[K23[m[K27.txt

Andy's PHP Projects Man Page Lookup Script - Information Disclosure
| php/webapps/[01;31m[K23[m[K536.txt

AnnonceV News Script 1.1 - 'page' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K05.txt

anteco visual technologies ownserver 1.0 - Directory Traversal
| windows/remote/[01;31m[K23[m[K560.txt

Antologic Antolinux 1.0 - Administrative Interface 'NDCR' Remote Command Execution | linux/remote/[01;31m[K23[m[K604.txt

Anuko Time Tracker 1.19.[01;31m[K23[m[K.5311 - No rate Limit on Password Reset functionality | php/webapps/49173.txt

Anuko Time Tracker 1.19.[01;31m[K23[m[K.5311 - Password Reset leading to Account Takeover | php/webapps/49174.txt

Anuko Time Tracker 1.19.[01;31m[K23[m[K.5325 - CSV/Formula Injection | php/webapps/49027.txt

AoA Audio Extractor 2.x - ActiveX ROP | windows/remote/15[01;31m[K23[m[K5.html

AOL Instant Messenger 4.x/5.x - Buddy Icon Predictable File Location | windows/remote/[01;31m[K23[m[K730.txt

Apache 2.0.4x mod_perl - File Descriptor Leakage (3) | linux/local/[01;31m[K23[m[K581.pl

Apache 2.0.4x mod_php - File Descriptor Leakage (1) | linux/local/[01;31m[K23[m[K481.c

Apache 2.0.4x mod_php - File Descriptor Leakage (2) | linux/local/[01;31m[K23[m[K482.c

Apache 2.4.[01;31m[K23[m[K mod_http2 - Denial of Service | linux/dos/40909.py

Apache < 1.3.37/2.0.59/2.2.3 mod_rewrite - Remote Overflow | multiple/remote/2[01;31m[K23[m[K7.sh

Apache cocoon 2.14/2.2 - Directory Traversal | multiple/remote/[01;31m[K23[m[K282.txt

Apache Cygwin 1.3.x/2.0.x - Directory Traversal | windows/remote/[01;31m[K23[m[K751.txt

Apache OFBiz - Multiple Cross-Site Scripting Vulnerabilities | php/webapps/1[01;31m[K23[m[K30.txt

Apache OFBiz 10.4.x - Multiple Cross-Site Scripting Vulnerabilities | multiple/remote/38[01;31m[K23[m[K0.txt

Apache Struts 2.3.x Showcase - Remote Code Execution | multiple/webapps/4[01;31m[K23[m[K24.py

Apache Superset < 0.[01;31m[K23[m[K - Remote Code Execution | linux/webapps/45933.py

```
Apache Tomcat 10.1.39 - Denial of Service (DoS)
| multiple/remote/5[01;31m[K23[m[K18.py

Apache Tomcat 4.0.x - Non-HTTP Request Denial of Service
| linux/dos/[01;31m[K23[m[K245.pl

Apache Tomcat 5.5.0 < 5.5.29 / 6.0.0 < 6.0.26 - Information Disclosure
| multiple/remote/1[01;31m[K23[m[K43.txt

Apache Tomcat 6.0.18 - Form Authentication Existing/Non-Existing
'Username' Enumeration                    |
multiple/remote/330[01;31m[K23[m[K.txt

Apache Tomcat < 9.0.1 (Beta) / < 8.5.[01;31m[K23[m[K / < 8.0.47 / <
7.0.8 - JSP Upload Bypass / Remote Code Execution ( |
jsp/webapps/42966.py

Apache Tomcat < 9.0.1 (Beta) / < 8.5.[01;31m[K23[m[K / < 8.0.47 / <
7.0.8 - JSP Upload Bypass / Remote Code Execution ( |
windows/webapps/42953.txt

Apache::Gallery 0.4/0.5/0.6 - Insecure File Storage Privilege
Escalation                                  |
linux/local/[01;31m[K23[m[K119.c

Apple Bonjour for Windows 1.0.4 - mDNSResponder Null Pointer
Dereference Denial of Service               |
windows/dos/3[01;31m[K23[m[K50.txt

Apple iChat Bonjour 3.1.6.441 - Multiple Denial of Service
Vulnerabilities                             |
osx/dos/3[01;31m[K23[m[K0.rb

Apple iOS 1.1.4/2.0 / iPod 1.1.4/2.0 touch Safari WebKit - 'alert()'
Remote Denial of Service              |
hardware/dos/3[01;31m[K23[m[K41.html

Apple iPhone 3.1.2 - '7D11' Model MB702LL Mobile Safari Denial of
Service                                 |
hardware/dos/1[01;31m[K23[m[K44.txt

Apple iTunes 9.0 - '.pls' Buffer Overflow
| osx/dos/33[01;31m[K23[m[K5.rb

Apple Mac OS Internet Explorer 3/4/5 - File Execution
| osx/remote/21[01;31m[K23[m[K8.txt

Apple Mac OSX 10 - CD9660.Util Probe For Mounting Argument Local Buffer
Overflow                          | osx/dos/[01;31m[K23[m[K442.txt

Apple Mac OSX 10.4.x - Software Update Format String
| osx/dos/295[01;31m[K23[m[K.txt
```

Apple Mac OSX 10.6 - HFS FileSystem (Denial of Service)
| osx/dos/1[01;31m[K23[m[K75.c

Apple Mac OSX 10.x - SecurityServer Daemon Local Denial of Service
| osx/dos/[01;31m[K23[m[K505.c

Apple Mac OSX Kernel - Null Pointer Dereference in
AppleGraphicsDeviceControl |
osx/dos/399[01;31m[K23[m[K.c

Apple Mac OSX xnu 1228.0 - 'super_blob' Local kernel Denial of Service
(PoC) | osx/dos/47[01;31m[K23[m[K.c

Apple macOS 10.12 16A3[01;31m[K23[m[K XNU Kernel / iOS 10.1.1 -
'set_dp_control_port' Lack of Locking Use-After-Free |
multiple/local/40931.txt

Apple macOS High Sierra 10.13 - 'ctl_ctloutput-leak' Information Leak
| macos/local/44[01;31m[K23[m[K4.c

Apple macOS Sierra 10.12.1 - 'IOFireWireFamily' FireWire Port Denial of
Service | macos/dos/44[01;31m[K23[m[K5.c

Apple macOS Sierra 10.12.1 - 'physmem' Local Privilege Escalation
| macos/local/44[01;31m[K23[m[K7.md

Apple macOS Sierra 10.12.3 - 'IOFireWireFamily-null-deref' FireWire
Port Denial of Service | macos/dos/44[01;31m[K23[m[K6.c

Apple OS X 10.10.5 - 'rootsh' Local Privilege Escalation
| osx/local/44[01;31m[K23[m[K9.md

Apple OS X Yosemite - 'flow_divert-heap-overflow' Kernel Panic
| osx/dos/44[01;31m[K23[m[K8.c

Apple QuickTime/Darwin Streaming Server 4.1.x - 'parse_xml.cgi' File
Disclosure |
cgi/remote/2[01;31m[K23[m[K12.txt

Apple Safari 1.x - Cookie Directory Traversal
| osx/remote/[01;31m[K23[m[K800.txt

Apple Safari 1.x - Large JavaScript Array Handling Denial of Service
| osx/dos/[01;31m[K23[m[K793.txt

Apple Safari For Windows - PhishingAlert Security Bypass
| windows/remote/389[01;31m[K23[m[K.txt

Applied Watch Command Center 1.0 - Authentication Bypass (1)
| multiple/remote/[01;31m[K23[m[K404.c

Applied Watch Command Center 1.0 - Authentication Bypass (2)
| multiple/remote/[01;31m[K23[m[K405.c

AppLocker - Execution Prevention Bypass (Metasploit)
| windows/local/395[01;31m[K23[m[K.rb

Aprox Portal 3.0 - File Disclosure
| php/webapps/[01;31m[K23[m[K630.txt

ArbitroWeb PHP Proxy 0.5/0.6 - Cross-Site Scripting
| php/webapps/24[01;31m[K23[m[K1.txt

argon client management services 1.31 - Directory Traversal
| windows/remote/5[01;31m[K23[m[K0.txt

ArGoSoft FTP Server 1.0/1.2/1.4 - Multiple Vulnerabilities
| windows/dos/[01;31m[K23[m[K769.pl

Array Networks vxAG 9.2.0.34 and vAPV 8.3.2.17 - Multiple
Vulnerabilities |
hardware/webapps/3[01;31m[K23[m[K69.txt

ArticlesOne 07[01;31m[K23[m[K2006 - 'page' Remote File Inclusion
| php/webapps/2063.txt

asgbookPHP 1.9 - 'index.php' Cross-Site Scripting
| php/webapps/36[01;31m[K23[m[K7.txt

Ashley Brown iWeb Server - Encoded Backslash Directory Traversal
| windows/remote/[01;31m[K23[m[K318.txt

ASP Portal - Multiple Vulnerabilities
| asp/webapps/[01;31m[K23[m[K696.pl

ASP-Nuke 1.0/1.2/1.3 - Remote User Database Access
| asp/webapps/[01;31m[K23[m[K516.txt

ASP2PHP 0.76.[01;31m[K23[m[K - Preparse Token Variable Buffer Overflow
| windows/remote/25016.txt

ASPApp PortalApp - Remote User Database Access
| asp/webapps/[01;31m[K23[m[K515.txt

ASPBB 0.4 - 'profile.asp?PROFILE_ID' SQL Injection
| asp/webapps/268[01;31m[K23[m[K.txt

ASPRunner.NET 10.1 - Denial of Service (PoC)
| windows/dos/468[01;31m[K23[m[K.py

Astium VoIP PBX 2.1 build 25399 - Multiple Vulnerabilities/Remote
Command Execution |
php/webapps/[01;31m[K23[m[K831.py

Astium VoIP PBX 2.1 build 25399 - Remote Crash (PoC)
| linux/dos/[01;31m[K23[m[K830.py

```
Atar2b CMS 4.0.1 - 'pageE.php?id' SQL Injection
| php/webapps/365[01;31m[K23[m[K.txt

Athena Web Registration - Remote Command Execution
| php/webapps/[01;31m[K23[m[K513.txt

Athttpd 0.4b - GET Remote Buffer Overrun
| linux/remote/[01;31m[K23[m[K188.c

ATKGFNEXSrv ATKGFNEX 1.0.11.1 - Unquoted Service Path Privilege
Escalation                                  |
windows/local/405[01;31m[K23[m[K.txt

AtomCMS - SQL Injection / Arbitrary File Upload
| php/webapps/39[01;31m[K23[m[K8.txt

Atomic Photo Album 0.x/1.0 - 'Apa_PHPInclude.INC.php' Remote File
Inclusion                                   |
php/webapps/260[01;31m[K23[m[K.txt

Atrise Everyfind 5.0.2 - search Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K207.txt

Atrium Software Mercur MailServer 3.3/4.0/4.2 - IMAP AUTH Remote Buffer
Overflow                           | windows/dos/[01;31m[K23[m[K267.txt

Attila PHP 3.0 - SQL Injection Unauthorized Privileged Access
| php/webapps/[01;31m[K23[m[K064.txt

AudioCoder (.lst) - Local Buffer Overflow (Metasploit)
| windows/local/265[01;31m[K23[m[K.rb

AudioCoder 0.8.46 - Local Buffer Overflow (SEH)
| windows/local/4[01;31m[K23[m[K85.py

Authentium SafeCentral 2.6 - 'shdrv.sys' Local Kernel Ring0 SYSTEM
| windows/local/11[01;31m[K23[m[K2.c

Auto Dealer - SQL Injection
| php/webapps/14[01;31m[K23[m[K9.txt

Automatic-Systems SOC FL9600 FastLine - Directory Transversal
| php/webapps/518[01;31m[K23[m[K.txt

Automic Agent 24.3.0 HF4 - Privilege Escalation
| multiple/remote/5[01;31m[K23[m[K09.txt

AvailScript Job Portal Script - 'applynow.php' SQL Injection
| php/webapps/3[01;31m[K23[m[K52.txt

Avant Browser 11.7 Build 9 - JavaScript Engine Integer Overflow
| multiple/dos/3[01;31m[K23[m[K81.js
```

Avant Browser 8.0.2 - 'HTTP Request' Buffer Overflow (PoC)
| multiple/dos/[01;31m[K23[m[K050.txt

Avast Anti-Virus < 19.1.[01;31m[K23[m[K60 - Local Credentials Disclosure |
windows/local/46345.py

Avaya Argent Office - DNS Packet Denial of Service
| windows/dos/[01;31m[K23[m[K337.c

Avaya Intuity Audix LX R1.1 - Multiple Remote Vulnerabilities
| cgi/webapps/33[01;31m[K23[m[K1.txt

AVCON H3[01;31m[K23[m[KCall - Local Buffer Overflow
| windows/local/12528.pl

AWCM 2.1 - Local File Inclusion / Authentication Bypass
| php/webapps/9[01;31m[K23[m[K7.txt

Axis Communications Video Server 2.x - 'Command.cgi' File Creation
| cgi/remote/2[01;31m[K23[m[K11.txt

Axway Secure Transport 5.1 SP2 - Directory Traversal
| windows/webapps/[01;31m[K23[m[K324.txt

AZBB < 1.0.07d - Multiple Vulnerabilities
| php/webapps/438[01;31m[K23[m[K.txt

AzDGDatingLite 2.1.1 - 'index.php?language' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K934.txt

AzDGDatingLite 2.1.1 - 'view.php?id' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K935.txt

Azure Apache Ambari [01;31m[K23[m[K02250400 - Spoofing
| multiple/remote/51546.py

B-Cumulus - 'tagcloud' Multiple Cross-Site Scripting Vulnerabilities
| multiple/webapps/35[01;31m[K23[m[K3.txt

Backdrop CMS 1.20.0 - 'Multiple' Cross-Site Request Forgery (CSRF)
| php/webapps/503[01;31m[K23[m[K.html

Backdrop CMS 1.[01;31m[K23[m[K.0 - Stored XSS
| php/webapps/51905.txt

BaconMap 1.0 - Local File Disclosure
| php/webapps/15[01;31m[K23[m[K4.txt

BaconMap 1.0 - SQL Injection
| php/webapps/15[01;31m[K23[m[K3.txt

Baidu Spark Browser 43.[01;31m[K23[m[K.1000.476 - Address Bar URL Spoofing |
windows/dos/39774.html

Baixar GLPI Project 9.4.6 - SQLi
| multiple/webapps/508[01;31m[K23[m[K.txt

Bajie HTTP Server 0.95 - Example Scripts and Servlets Cross-Site Scripting |
multiple/remote/[01;31m[K23[m[K257.txt

banana dance b.2.6 - Multiple Vulnerabilities
| php/webapps/[01;31m[K23[m[K573.txt

BandSite CMS 1.1 - 'bio_content.php' Cross-Site Scripting
| php/webapps/286[01;31m[K23[m[K.txt

Barracuda Load Balancer Firmware < 6.0.1.006 - Remote Command Injection (Metasploit) |
hardware/webapps/4[01;31m[K23[m[K33.rb

Barracuda Spam Firewall < 3.1.18 - Command Execution (Metasploit)
| cgi/webapps/1[01;31m[K23[m[K6.pm

Barracuda Web Application Firewall 660 - '/cgi-mod/index.cgi' Multiple HTML Injection Vulnerabilities |
hardware/remote/334[01;31m[K23[m[K.txt

BASE 1.2.4 - melissa Snort Frontend Remote File Inclusion
| php/webapps/18[01;31m[K23[m[K.txt

Basic Analysis and Security Engine (BASE) 1.4.5 - '/setup/setup2.php?ado_inc_PHP' Remote File Inclusion |
php/webapps/367[01;31m[K23[m[K.txt

Basit 1.0 Search Module - Cross-Site Scripting
| php/webapps/2[01;31m[K23[m[K85.txt

Basit 1.0 Submit Module - Cross-Site Scripting
| php/webapps/2[01;31m[K23[m[K83.txt

BBlog 0.7.6 - 'mod' SQL Injection
| php/webapps/6[01;31m[K23[m[K3.txt

bcoos 1.0.10 - 'ratephoto.php' SQL Injection
| php/webapps/308[01;31m[K23[m[K.txt

BCWB 0.99 - 'ROOT_PATH' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K99.txt

BEA Tuxedo 6/7/8 and WebLogic Enterprise 4/5 - Input Validation
| cgi/remote/[01;31m[K23[m[K312.txt

BEA WebLogic 6/7/8 - InteractiveQuery.jsp Cross-Site Scripting
| jsp/webapps/[01;31m[K23[m[K315.txt

Beautifier 0.1 - 'Core.php' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K14.txt

Beehive Forum - Account Takeover
| php/webapps/509[01;31m[K23[m[K.py

Beehive Forum 0.6.2 - Multiple HTML Injection Vulnerabilities
| php/webapps/269[01;31m[K23[m[K.txt

Belchior Foundry VCard 2.8 - Authentication Bypass
| php/webapps/[01;31m[K23[m[K843.txt

Belkin F5D7[01;31m[K23[m[K4-4 v5 G Wireless Router - Remote Hash
Exposed |
hardware/webapps/17349.txt

Belkin F5D8[01;31m[K23[m[K3-4 Wireless N Router (Multiple Scripts) -
Authentication Bypass |
hardware/remote/32582.txt

Belkin F5D8[01;31m[K23[m[K6-4 Router - Cross-Site Request Forgery
| hardware/remote/38495.html

Belkin F5D9[01;31m[K23[m[K0-4 Wireless G Plus MIMO Router -
Authentication Bypass |
hardware/remote/4941.txt

Belkin F7D7601 NetCam - Multiple Vulnerabilities
| hardware/remote/4[01;31m[K23[m[K31.txt

BES-CMS 0.4/0.5 - '/members/index.inc.php' File Inclusion
| php/webapps/[01;31m[K23[m[K454.txt

BES-CMS 0.4/0.5 - 'folder.php' File Inclusion
| php/webapps/[01;31m[K23[m[K457.txt

BES-CMS 0.4/0.5 - 'hacking.php' File Inclusion
| php/webapps/[01;31m[K23[m[K458.txt

BES-CMS 0.4/0.5 - 'index.inc.php' File Inclusion
| php/webapps/[01;31m[K23[m[K453.txt

BES-CMS 0.4/0.5 - 'message.php' File Inclusion
| php/webapps/[01;31m[K23[m[K455.txt

BES-CMS 0.4/0.5 - 'start.php' File Inclusion
| php/webapps/[01;31m[K23[m[K456.txt

Better Basket Pro 3.0 Store Builder - Full Path Disclosure
| php/webapps/[01;31m[K23[m[K010.txt

BigTree 4.3.4 CMS - Multiple SQL Injection
| php/webapps/466[01;31m[K23[m[K.txt

BigTree CMS 4.2.[01;31m[K23[m[K - Cross-Site Scripting
| php/webapps/45628.txt

BIND 9.5.0-P2 - 'Randomized Ports' Remote DNS Cache Poisoning
| multiple/remote/6[01;31m[K23[m[K6.txt

BIND 9.x - Remote DNS Cache Poisoning
| multiple/remote/61[01;31m[K23[m[K.py

BinGo News 3.01 - 'bnrep' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K12.txt

BirthSys 3.1 - Multiple SQL Injections
| php/webapps/27[01;31m[K23[m[K9.txt

BitchX 1.0 - Remote 'Send_CTCP()' Memory Corruption
| linux/remote/2[01;31m[K23[m[K53.c

Bitfolge Snif 1.2.6 - 'index.php' Path Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K420.txt

BlackBoard Academic Suite 6.2.3.[01;31m[K23[m[K - Frameset.jsp Cross-Domain Frameset Loading |
jsp/webapps/26778.txt

BlackBoard Learning System 5.x/6.0 - Multiple Cross-Site Scripting Vulnerabilities |
cgi/webapps/[01;31m[K23[m[K986.txt

Blaxxun Contact 3D - X-CC3D Browser Object Buffer Overflow (PoC)
| windows/dos/[01;31m[K23[m[K916.txt

BlazeDVD 6.1 - '.PLF' File (ASLR + DEP Bypass) (Metasploit)
| windows/local/[01;31m[K23[m[K783.rb

BlazeVideo HDTV Player Pro 6.6 - Filename Handling (Metasploit)
| windows/local/[01;31m[K23[m[K052.rb

Blog:CMS 4.1.3 - 'NP_UserSharing.php' Remote File Inclusion
| php/webapps/29[01;31m[K23[m[K.txt

Bloo 1.00 - Multiple SQL Injections
| php/webapps/5[01;31m[K23[m[K4.txt

BM Classifieds 20080409 - Multiple SQL Injections
| php/webapps/52[01;31m[K23[m[K.txt

BolinOS 4.5.5 - 'gBRootPath' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K72.txt

BolinTech DreamFTP Server 1.0 - User Name Format String
| windows/dos/[01;31m[K23[m[K660.c

BolinTech DreamFTP Server 1.2 (1.02/TryFTP 1.0.0.1) - Remote User Name
Format String | windows/remote/8[01;31m[K23[m[K.c

Book Store Management System 1.0.0 - Stored Cross-Site Scripting (XSS)
| php/webapps/511[01;31m[K23[m[K.txt

borland Web server for corel paradox 1.0 b3 - Directory Traversal
| windows/remote/[01;31m[K23[m[K597.txt

BosDev BosDates 3.x - SQL Injection
| php/webapps/[01;31m[K23[m[K685.txt

BrewBlogger 2.1.0.1 - Arbitrary Add Admin
| php/webapps/60[01;31m[K23[m[K.pl

Broadcom Wi-Fi Devices - 'KR00K Information Disclosure
| multiple/remote/48[01;31m[K23[m[K3.py

BRS Webweaver 1.0.7 - 'ISAPISkeleton.dll' Cross-Site Scripting
| windows/remote/[01;31m[K23[m[K612.txt

BRS Webweaver 1.06 - HTTPd 'User-Agent' Remote Denial of Service
| multiple/dos/[01;31m[K23[m[K325.c

BS Auction - SQL Injection
| php/webapps/14[01;31m[K23[m[K8.txt

Bs Auction Script - SQL Injection
| php/webapps/14[01;31m[K23[m[K3.txt

Bs Business_Directory Script - SQL Injection / Authentication Bypass
| php/webapps/14[01;31m[K23[m[K0.txt

Bs Scripts_Directory - SQL Injection / Authentication Bypass
| php/webapps/142[01;31m[K23[m[K.txt

BSA Radar 1.6.7[01;31m[K23[m[K4.24750 - Authenticated Privilege
Escalation |
multiple/webapps/48649.txt

BSA Radar 1.6.7[01;31m[K23[m[K4.24750 - Cross-Site Request Forgery
(Change Password) |
hardware/webapps/48653.txt

BSA Radar 1.6.7[01;31m[K23[m[K4.24750 - Local File Inclusion
| multiple/webapps/48666.txt

BSA Radar 1.6.7[01;31m[K23[m[K4.24750 - Persistent Cross-Site Scripting
| multiple/webapps/48619.txt

BSD 'lpr' 2000.05.07/0.48/0.72 / lpr-ppd 0.72 - Local Buffer Overflow (1) | unix/local/2[01;31m[K23[m[K31.c

BSD 'lpr' 2000.05.07/0.48/0.72 / lpr-ppd 0.72 - Local Buffer Overflow (2) | unix/local/2[01;31m[K23[m[K32.c

BSD - SHMAT System Call Privilege Escalation
| bsd/local/[01;31m[K23[m[K655.txt

BSD-Games 2.x - Monop Player Name Local Buffer Overrun (1)
| bsd/local/[01;31m[K23[m[K062.c

BSD-Games 2.x - Monop Player Name Local Buffer Overrun (2)
| bsd/local/[01;31m[K23[m[K063.c

BSD/Linux Kernel 2.3 (BSD/OS 4.0 / FreeBSD 3.2 / NetBSD 1.4) - Shared Memory Denial of Service | bsd/dos/194[01;31m[K23[m[K.c

BT Voyager 2000 Wireless ADSL Router - SNMP Community String Information Disclosure |
hardware/remote/24[01;31m[K23[m[K0.txt

Budget Management System 1.0 - 'Budget title' Stored XSS
| php/webapps/497[01;31m[K23[m[K.txt

BulletScript MailList - bsml.pl Information Disclosure
| cgi/webapps/[01;31m[K23[m[K488.txt

Bus Pass Management System 1.0 - 'viewid' SQL Injection
| php/webapps/50[01;31m[K23[m[K5.txt

Bytehoard 0.7 - File Disclosure
| php/webapps/[01;31m[K23[m[K261.txt

C-News 1.0.1 - 'path' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K08.txt

Cacheflow CacheOS 4.1.10016 - HTTP HOST Proxy
| multiple/remote/[01;31m[K23[m[K137.txt

Cacti 0.8.7e - Multiple Vulnerabilities
| php/webapps/10[01;31m[K23[m[K4.txt

Cacti 0.8.7e - OS Command Injection
| php/webapps/1[01;31m[K23[m[K39.txt

Cacti 0.8.7e - SQL Injection
| php/webapps/1[01;31m[K23[m[K38.txt

CactuShop - User Invoices Persistent Cross-Site Scripting
| asp/webapps/1[01;31m[K23[m[K29.txt

```
CactuSoft CactuShop 5.0/5.1 - Cross-Site Scripting
| asp/webapps/[01;31m[K23[m[K899.txt

Cactusoft CactuShop 5.0/5.1 - SQL Injection
| asp/webapps/[01;31m[K23[m[K898.txt

Cadre PHP Framework - Remote File Inclusion
| php/webapps/3[01;31m[K23[m[K7.txt

Cain & Abel 4.9.[01;31m[K23[m[K - '.rdp' Buffer Overflow (PoC)
| windows/dos/7297.py

Cain & Abel 4.9.[01;31m[K23[m[K - '.rdp' Local Buffer Overflow
| windows/local/7329.py

calacode @mail webmail system 3.52 - Multiple Vulnerabilities
| cgi/webapps/[01;31m[K23[m[K421.txt

Caldera UnixWare 7.1.1 - WebTop 'SCOAdminReg.cgi' Arbitrary Command
Execution                                |
unixware/local/21[01;31m[K23[m[K9.sh

Calendarix 0.7.20070307 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/30[01;31m[K23[m[K2.txt

Calendarix 0.7.20070307 - Multiple SQL Injections
| php/webapps/30[01;31m[K23[m[K4.txt

Campcodes Online Hospital Management System 1.0 - SQL Injection
| multiple/webapps/5[01;31m[K23[m[K12.txt

carey internets services commerce.cgi 2.0.1 - Directory Traversal
| cgi/remote/206[01;31m[K23[m[K.txt

Cars & Vehicle - 'page.php' SQL Injection
| php/webapps/3[01;31m[K23[m[K88.txt

Caucho Resin 2.0/2.1 - Multiple HTML Injection / Cross-Site Scripting
Vulnerabilities                      |
jsp/webapps/[01;31m[K23[m[K262.txt

Caucho Technology Resin 2.1.12 - Directory Listings Disclosure
| linux/remote/[01;31m[K23[m[K671.txt

Cauldron Chaser 1.4/1.5 - Remote Denial of Service (1)
| multiple/dos/[01;31m[K23[m[K641.txt

Cauldron Chaser 1.4/1.5 - Remote Denial of Service (2)
| multiple/dos/[01;31m[K23[m[K642.txt

Cayman 3220-H DSL Router 1.0/GatorSurf 5.3 - Denial of Service
| hardware/dos/199[01;31m[K23[m[K.txt
```

```
CCleague Pro 1.0.1RC1 - 'cookie' Remote Code Execution
| php/webapps/[01;31m[K23[m[K33.php

CDex 1.70b2 (Windows XP SP3) - '.ogg' Local Buffer Overflow
| windows/local/8[01;31m[K23[m[K1.php

CDP 0.33/0.4 - Console CD Player PrintTOC Function Buffer Overflow
| hardware/dos/[01;31m[K23[m[K900.txt

CeleronDude Uploader 6.1 - 'account.php' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K34.txt

CentOS Control Web Panel 0.9.8.836 - Authentication Bypass
| linux/webapps/471[01;31m[K23[m[K.txt

Centreon Enterprise Server 2.3.3 < 2.3.9-4 - Blind SQL Injection
| php/webapps/[01;31m[K23[m[K362.py

Centrify Deployment Manager 2.1.0.283 - Local Privilege Escalation
| linux/local/[01;31m[K23[m[K251.txt

Centrinity FirstClass Desktop Client 7.1 - Local Buffer Overflow
| windows/local/[01;31m[K23[m[K921.c

Centrinity FirstClass HTTP Server 5.50/5.77/7.0/7.1 - Long Version
Field Denial of Service                  |
windows/dos/[01;31m[K23[m[K[01;31m[K23[m[K4.c

Centrinity FirstClass HTTP Server 5/7 - 'TargetName' Cross-Site
Scripting                                   |
windows/remote/[01;31m[K23[m[K871.txt

Centrinity FirstClass HTTP Server 7.1 - Directory Disclosure
| multiple/remote/[01;31m[K23[m[K309.txt

CenturyLink ZyXEL PK5001Z Router - Root Remote Code Execution
| hardware/remote/4[01;31m[K23[m[K55.c

Cerbere Proxy Server 1.2 - Long Host Header Field Remote Denial of
Service                                  |
multiple/dos/244[01;31m[K23[m[K.txt

Cerberus FTPServer 1.71/2.1/2.32 - Remote Denial of Service
| windows/dos/[01;31m[K23[m[K042.pl

CGIScript.net CSFAQ 1.0 Script - Full Path Disclosure
| cgi/webapps/24[01;31m[K23[m[K7.txt

CGIWrap 2.x/3.x - Cross-Site Scripting
| cgi/remote/210[01;31m[K23[m[K.txt

Chamillo LMS 1.11.8 - Arbitrary File Upload
| php/webapps/474[01;31m[K23[m[K.txt
```

Charon Cart 3.0 - 'Review.asp' SQL Injection
| asp/webapps/[01;31m[K23[m[K87.txt

Chasys Media Player 1.1 - '.m3u' Local Stack Overflow
| windows/local/8[01;31m[K23[m[K5.py

Chasys Media Player 1.1 - '.pls' Local Buffer Overflow (PoC) (SEH)
| windows/dos/8[01;31m[K23[m[K2.py

Chasys Media Player 1.1 - '.pls' Local Stack Overflow
| windows/local/8[01;31m[K23[m[K3.py

Chasys Media Player 1.1 - '.pls' Local Stack Overflow (2)
| windows/local/8[01;31m[K23[m[K4.py

ChatZilla 0.8.[01;31m[K23[m[K - Remote Denial of Service
| windows/dos/[01;31m[K23[m[K150.c

Check Point Connectra R62 - '/Login/Login' Arbitrary Script Injection
| hardware/remote/33[01;31m[K23[m[K4.txt

Check Point Firewall-1 4.x - SecuRemote Internal Interface Address
Information Leakage |
hardware/dos/[01;31m[K23[m[K087.c

Check Point FW-1 Syslog Daemon - Unfiltered Escape Sequence
| hardware/remote/2[01;31m[K23[m[K94.txt

Check Point UTM-1 Edge and Safe 8.2.43 - Multiple Vulnerabilities
| hardware/remote/36[01;31m[K23[m[K9.txt

Check Point VPN-1/FireWall-1 4.1 SP2 - Blocked Port Bypass
| windows/remote/[01;31m[K23[m[K2.c

Cherokee 0.1.x/0.2.x/0.4.x - Error Page Cross-Site Scripting
| solaris/remote/[01;31m[K23[m[K605.txt

Chi Kien Uong Guestbook 1.51 - Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K294.txt

Chinput 3.0 - Environment Variable Buffer Overflow
| linux/local/21[01;31m[K23[m[K1.c

Chipmunk Pwngame - Multiple SQL Injections
| php/webapps/152[01;31m[K23[m[K.txt

CHIYU TCP/IP Converter devices - CRLF injection
| cgi/webapps/499[01;31m[K23[m[K.txt

Cisco 871 Integrated Services Router - Cross-Site Request Forgery (1)
| hardware/remote/3[01;31m[K23[m[K90.html

Cisco 871 Integrated Services Router - Cross-Site Request Forgery (2)
| hardware/remote/3[01;31m[K23[m[K91.html

Cisco Adaptive Security Appliance Software 9.7 - Unauthenticated
Arbitrary File Deletion |
hardware/webapps/487[01;31m[K23[m[K.sh

Cisco ASA Software 8.x/9.x - IKEv1 / IKEv2 Buffer Overflow
| hardware/remote/398[01;31m[K23[m[K.py

Cisco DPC2100 - Denial of Service
| hardware/dos/215[01;31m[K23[m[K.txt

Cisco DPC2420 - Multiples Vulnerabilities
| hardware/webapps/[01;31m[K23[m[K250.txt

Cisco IOS 12 - Software '?/' HTTP Request Denial of Service
| hardware/dos/203[01;31m[K23[m[K.txt

Cisco IOS 12 MSFC2 - Layer 2 Frame Denial of Service
| hardware/dos/[01;31m[K23[m[K638.pl

Cisco IOS 12.4([01;31m[K23[m[K) - HTTP Server Multiple Cross-Site
Scripting Vulnerabilities |
hardware/remote/32776.txt

Cisco IOS 12.x - Firewall Authentication Proxy Buffer Overflow
| hardware/dos/26[01;31m[K23[m[K3.txt

Cisco IOS 12.x - HTTP Server Multiple Cross-Site Scripting
Vulnerabilities |
hardware/remote/327[01;31m[K23[m[K.txt

Cisco LEAP - Password Disclosure
| hardware/remote/[01;31m[K23[m[K212.txt

Cisco PIX Firewall 4.x/5.x - SMTP Content Filtering Evasion
| hardware/remote/20[01;31m[K23[m[K1.txt

Cisco Secure ACS for Windows NT 2.42 - Remote Buffer Overflow
| windows/remote/20[01;31m[K23[m[K5.pl

Cisco Unified Communications Manager - TFTP Service
| hardware/local/30[01;31m[K23[m[K7.sh

Cisco Wireless Lan Controller 7.2.110.0 - Multiple Vulnerabilities
| hardware/dos/[01;31m[K23[m[K361.txt

Citadel/UX 6.[01;31m[K23[m[K - Remote USER Directive
| linux/remote/437.c

Citrix CloudBridge - 'CAKEPHP' Cookie Command Injection
| cgi/webapps/4[01;31m[K23[m[K46.txt

Citrix Metaframe XP - Cross-Site Scripting
| windows/remote/[01;31m[K23[m[K316.txt

Citrix Nfuse 1.6 - Published Applications Information Leak
| windows/remote/21[01;31m[K23[m[K5.pl

City Directory Review and Rating Script - 'search.php' SQL Injection
| php/webapps/[01;31m[K23[m[K6[01;31m[K23[m[K.txt

CJ Ultra Plus 1.0.3/1.0.4 - 'OUT.php' SQL Injection
| php/webapps/256[01;31m[K23[m[K.txt

ClamAV Daemon 0.65 - UUEncoded Message Denial of Service
| linux/dos/[01;31m[K23[m[K667.txt

Class Scheduling System 1.0 - Multiple Stored XSS
| php/webapps/493[01;31m[K23[m[K.txt

Claymore Dual ETH + DCR/SC/LBC/PASC GPU Miner - Stack Buffer Overflow / Path Traversal |
windows/remote/43[01;31m[K23[m[K1.py

Clean CMS 1.5 - Blind SQL Injection
| php/webapps/7[01;31m[K23[m[K0.pl

Clearswift MAILsweeper 4.x - MIME Attachment Filter Bypass
| windows/remote/2[01;31m[K23[m[K38.txt

Clickcess ChitChat.NET - name Cross-Site Scripting
| asp/webapps/[01;31m[K23[m[K032.txt

Clickcess ChitChat.NET - topic title Cross-Site Scripting
| asp/webapps/[01;31m[K23[m[K033.txt

clipak - Arbitrary File Upload
| php/webapps/1[01;31m[K23[m[K83.txt

Clipbucket 2.6 Revision 738 - Multiple SQL Injections
| php/webapps/[01;31m[K23[m[K252.txt

Cloisterblog 1.2.2 - Journal.pl Directory Traversal
| cgi/webapps/[01;31m[K23[m[K894.txt

CloudClassroom PHP Project 1.0 - SQL Injection
| php/webapps/5[01;31m[K23[m[K14.txt

CLScript.com Classifieds Software - SQL Injection
| php/webapps/124[01;31m[K23[m[K.txt

cms (id) 5.0 - SQL Injection
| php/webapps/1[01;31m[K23[m[K33.txt

```
CMS Ariadna 2009 - SQL Injection
| php/webapps/1[01;31m[K23[m[K01.txt

CMS Firebrand Tec - Local File Inclusion
| php/webapps/1[01;31m[K23[m[K78.txt

CMS Ortus 1.13 - SQL Injection
| php/webapps/7[01;31m[K23[m[K7.txt

CMScout 1.[01;31m[K23[m[K - 'index.php' SQL Injection
| php/webapps/4182.txt

CMtextS 1.0 - '/users_logins/admin.txt' Credentials Disclosure
| php/webapps/[01;31m[K23[m[K88.txt

Cockpit Version [01;31m[K23[m[K4 - Server-Side Request Forgery
(Unauthenticated)                                          |
multiple/webapps/49397.txt

CoffeeCup Software Password Wizard 4.0 - HTML Source Password Retrieval
| windows/local/2[01;31m[K23[m[K29.c

Colloquy 1.3.5/1.3.6 - Denial of Service
| hardware/dos/240[01;31m[K23[m[K.py

ColoradoFTP 1.3 Prime Edition (Build 8) - Directory Traversal
| java/webapps/40[01;31m[K23[m[K1.txt

Comcast DOCSIS 3.0 Business Gateways - Multiple Vulnerabilities
| hardware/remote/161[01;31m[K23[m[K.txt

COMMAX UMS Client ActiveX Control 1.7.0.2 - 'CNC_Ctrl.dll' Heap Buffer
Overflow                              |
hardware/webapps/50[01;31m[K23[m[K2.txt

COMMAX WebViewer ActiveX Control 2.1.4.5 - 'Commax_WebViewer.ocx'
Buffer Overflow                            |
hardware/webapps/50[01;31m[K23[m[K1.txt

CommerceSQL Shopping Cart 2.2 - 'index.cgi' Directory Traversal
| cgi/webapps/[01;31m[K23[m[K395.txt

Community CMS 0.5 - Multiple SQL Injections
| php/webapps/83[01;31m[K23[m[K.txt

CommVault Edge 11 SP6 - Stack Buffer Overflow (PoC)
| windows/dos/418[01;31m[K23[m[K.py

CommView 6.1 (Build 636) - Local Blue Screen of Death (Denial of
Service)                                    |
windows/dos/1[01;31m[K23[m[K56.c
```

Compaq Client Management Agents 3.70/4.0 / Insight Management Agents 4.21 A/4.22 A/4.30 A / Intelligent Cl | multiple/dos/19225.txt

Compaq Web-Based Management Agent - Access Violation Denial of Service | windows/dos/228[01;31m[K23[m[K.txt

Confixx 2 - 'DB' SQL Injection
| php/webapps/[01;31m[K23[m[K797.txt

Confixx 2 - Perl Debugger Remote Command Execution
| php/webapps/[01;31m[K23[m[K798.txt

Confixx 3.0/3.1 - 'FTP_index.php' Cross-Site Scripting
| php/webapps/280[01;31m[K23[m[K.txt

ContentKeeper Web - Remote Command Execution (Metasploit)
| hardware/webapps/169[01;31m[K23[m[K.rb

CoolForum 0.5/0.7/0.8 - 'avatar.php?img' Cross-Site Scripting
| php/webapps/25[01;31m[K23[m[K9.txt

Coppermine Photo Gallery 1.2.2b (Nuke Addon) - Remote File Inclusion
| php/webapps/[01;31m[K23[m[K75.txt

Corel Linux OS 1.0 - get_it PATH
| linux/local/197[01;31m[K23[m[K.txt

Coreutils 4.5.x - LS Width Argument Integer Overflow
| linux/dos/[01;31m[K23[m[K274.pl

Counter Strike: Condition Zero - '.BSP' Map File Code Execution
| windows/local/4[01;31m[K23[m[K25.py

cPanel 11 BoxTrapper - Manage.HTML Cross-Site Scripting
| php/webapps/29[01;31m[K23[m[K7.txt

cPanel 5/6/7/8/9 - 'dir' Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K806.txt

cPanel 5/6/7/8/9 - Login Script Remote Command Execution
| cgi/webapps/[01;31m[K23[m[K807.txt

cPanel 5/6/7/8/9 - Resetpass Remote Command Execution
| cgi/remote/[01;31m[K23[m[K804.txt

cPanel Web Hosting Manager 3.1 - Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/29[01;31m[K23[m[K8.txt

Crackalaka IRC Server 1.0.8 - Remote Denial of Service
| linux/dos/[01;31m[K23[m[K943.txt

```
Crob FTP Server 3.5.1 - Denial of Service
| windows/dos/[01;31m[K23[m[K633.txt

Crob FTP Server 3.5.1 - Remote Information Disclosure
| windows/remote/[01;31m[K23[m[K632.txt

Crob FTP Server 3.5.2 - Remote Denial of Service
| windows/dos/[01;31m[K23[m[K689.c

Crystal Reports CrystalPrintControl - ActiveX ServerResourceVersion
Property Overflow (Metasploit)         |
windows/remote/[01;31m[K23[m[K472.rb

CUPS < 2.0.3 - Remote Command Execution
| linux/remote/41[01;31m[K23[m[K3.py

CuteFTP Mac 3.1 - Denial of Service (PoC)
| macos/dos/458[01;31m[K23[m[K.py

CuteNews 0.88/1.3 - 'example1.php' Cross-Site Scripting
| php/webapps/24[01;31m[K23[m[K8.txt

CuteNews 0.88/1.3 - 'example2.php' Cross-Site Scripting
| php/webapps/24[01;31m[K23[m[K9.txt

CuteNews 1.3 - Debug Query Information Disclosure
| php/webapps/[01;31m[K23[m[K406.txt

CVE-20[01;31m[K23[m[K-50071 - Multiple SQL Injection
| php/webapps/51862.txt

CVSTrac 2.0.0 - Defacement Denial of Service
| cgi/dos/32[01;31m[K23[m[K.pl

CyberArk PSMP 10.9.1 - Policy Restriction Bypass
| multiple/remote/48[01;31m[K23[m[K9.txt

CyberArk Viewfinity 5.5.10.95 - Local Privilege Escalation
| windows/local/4[01;31m[K23[m[K19.txt

Cyberoam SSLVPN Client 1.3.1.30 - 'Connect To Server' Denial of Service
(PoC)                              | windows/dos/469[01;31m[K23[m[K.py

CyberPanel 2.1 - Remote Code Execution (RCE) (Authenticated)
| multiple/webapps/50[01;31m[K23[m[K0.py

Cyberstop Web Server 0.1 - Long Request Denial of Service
| windows/dos/21[01;31m[K23[m[K7.pl

CyberStrong eShop 4.2 - '10expand.asp' SQL Injection
| asp/webapps/259[01;31m[K23[m[K.txt
```

```
Cyrus IMSP Daemon 1.x - Remote Buffer Overflow
| linux/remote/[01;31m[K23[m[K441.c

Cythosia 2.x Botnet (C2 Web Panel) - SQL Injection
| php/webapps/30[01;31m[K23[m[K8.txt

D-Link Airspot DSA-3100 Gateway - 'Login_error.SHTML' Cross-Site
Scripting                                  |
hardware/remote/279[01;31m[K23[m[K.txt

D-Link DIR-100 1.12 - Security Bypass
| hardware/remote/3[01;31m[K23[m[K36.txt

D-Link DIR-600L AX 1.00 - Cross-Site Request Forgery
| hardware/webapps/3[01;31m[K23[m[K85.txt

D-Link DIR-615 - Multiple Buffer Overflow Vulnerabilities
| hardware/remote/387[01;31m[K23[m[K.txt

D-Link DNS-3[01;31m[K23[m[K - Multiple Vulnerabilities
| hardware/webapps/25142.txt

D-Link DSL-2740B - Multiple Cross-Site Request Forgery Vulnerabilities
| hardware/webapps/28[01;31m[K23[m[K9.txt

D-Link DSL-2780B DLink_1.01.14 - Remote DNS Change
| hardware/webapps/37[01;31m[K23[m[K7.txt

D-Link Routers - UPNP Buffer Overflow
| hardware/dos/28[01;31m[K23[m[K0.txt

D-Link WBR-[01;31m[K23[m[K10 1.0.4 - 'GET' Remote Buffer Overflow (PoC)
| hardware/dos/34394.pl

dagger Web engine [01;31m[K23[m[Kjan2007 - Remote File Inclusion
| php/webapps/4097.txt

DameWare Mini Remote Control Server 3.7x - Buffer Overflow (1)
| windows/remote/[01;31m[K23[m[K435.c

DameWare Mini Remote Control Server 3.7x - Buffer Overflow (2)
| windows/remote/[01;31m[K23[m[K436.c

DameWare Mini Remote Control Server 3.7x - Buffer Overflow (3)
| windows/remote/[01;31m[K23[m[K437.c

Danneo CMS 0.5.1 - Blind SQL Injection
| php/webapps/5[01;31m[K23[m[K9.php

DansGuardian 2.2.x - Denied URL Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K275.txt
```

DansGuardian Webmin Module 0.x - 'edit.cgi' Directory Traversal
| cgi/webapps/[01;31m[K23[m[K535.txt

Dansie Shopping Cart - Server Error Message Installation Full Path Disclosure |
cgi/webapps/[01;31m[K23[m[K266.txt

Darkwet Network WebcamXP 1.6.945 - Cross-Site Scripting
| multiple/remote/[01;31m[K23[m[K563.txt

Dasan Networks GPON ONT WiFi Router H64X Series - Authentication Bypass
| hardware/webapps/4[01;31m[K23[m[K20.txt

Dasan Networks GPON ONT WiFi Router H64X Series - Configuration Download |
hardware/webapps/4[01;31m[K23[m[K[01;31m[K23[m[K.txt

Dasan Networks GPON ONT WiFi Router H64X Series - Cross-Site Request Forgery |
hardware/webapps/4[01;31m[K23[m[K21.txt

Dasan Networks GPON ONT WiFi Router H64X Series - Privilege Escalation
| hardware/webapps/4[01;31m[K23[m[K22.txt

DataTaker DT80 dEX 1.50.012 - Information Disclosure
| hardware/webapps/4[01;31m[K23[m[K13.txt

DATEV Nutzungskontrolle 2.1/2.2 - Unauthorized Access
| windows/local/[01;31m[K23[m[K327.txt

dcam webcam server personal Web server 8.2.5 - Directory Traversal
| windows/remote/[01;31m[K23[m[K461.txt

DCForum+ 1.2 - 'Subject' HTML Injection
| php/webapps/[01;31m[K23[m[K008.txt

DCP-Portal 5.3.1 - 'calendar.php' Cross-Site Scripting
| php/webapps/2[01;31m[K23[m[K87.txt

DCP-Portal 5.5 - 'advertiser.php?Password' SQL Injection
| php/webapps/[01;31m[K23[m[K205.txt

DCP-Portal 5.5 - 'lostpassword.php?email' SQL Injection
| php/webapps/[01;31m[K23[m[K206.txt

DD-WRT 457[01;31m[K23[m[K - UPNP Buffer Overflow (PoC)
| hardware/dos/49730.py

DeDeCMS < 5.7-sp1 - Remote File Inclusion
| php/webapps/374[01;31m[K23[m[K.txt

Dell TrueMobile 1300 WLAN System 3.10.39.0 Tray Applet - Local Privilege Escalation | windows/local/[01;31m[K23[m[K739.txt

Dell TrueMobile [01;31m[K23[m[K00 - Remote Credential Reset | cgi/webapps/26761.txt

DELTAScripts PHP Classifieds 7.5 - Authentication Bypass | php/webapps/70[01;31m[K23[m[K.txt

Demo4 CMS 1b - 'FCKeditor' Arbitrary File Upload | php/webapps/59[01;31m[K23[m[K.pl

DeskPro 1.1 - Multiple SQL Injections | php/webapps/[01;31m[K23[m[K264.txt

DeskSoft CheckMail 1.2 - Password Disclosure | windows/local/[01;31m[K23[m[K041.txt

Digi Online Examination System 2.0 - Unrestricted Arbitrary File Upload | php/webapps/352[01;31m[K23[m[K.txt

DigiLIBE - Execution-After-Redirect Information Disclosure | php/webapps/38[01;31m[K23[m[K4.txt

Digital Audio Editor 7.6.0.[01;31m[K23[m[K7 - Local Crash (PoC) | windows/dos/15738.pl

Digital Reality Game Engine 1.0.x - Remote Denial of Service | windows/dos/[01;31m[K23[m[K752.c

Digital Scribe 1.x - Error Function Cross-Site Scripting | php/webapps/[01;31m[K23[m[K103.txt

Digital WebShop 1.128 - Multiple Remote File Inclusions | php/webapps/[01;31m[K23[m[K98.txt

DIMIN Viewer 5.4.0 - Crash (PoC) | windows/dos/[01;31m[K23[m[K279.py

DIMIN Viewer 5.4.0 - GIF Decode Crash (PoC) | windows/dos/[01;31m[K23[m[K496.txt

Discuz! 2.0/3.0 - Cross-Site Scripting | php/webapps/[01;31m[K23[m[K653.txt

Disk Pulse Server 2.2.34 - Remote Buffer Overflow | windows/remote/15[01;31m[K23[m[K8.py

DiskBoss Enterprise 8.2.14 - Remote Buffer Overflow | windows/remote/4[01;31m[K23[m[K95.py

DivFix++ 0.34 - Denial of Service
| linux/dos/4[01;31m[K23[m[K96.txt

Divine Content Server 5.0 - Error Page Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K217.txt

DNRD 1.x/2.x - DNS Request/Reply Denial of Service
| unix/dos/21[01;31m[K23[m[K6.txt

Docker Daemon - Unprotected TCP Socket
| linux/local/4[01;31m[K23[m[K56.txt

DokuWiki 2006-03-09b - 'dwpage.php' Remote Code Execution
| php/webapps/[01;31m[K23[m[K21.php

DokuWiki 2006-03-09b - 'dwpage.php' System Disclosure
| php/webapps/[01;31m[K23[m[K22.php

Dol Storye - 'Dettaglio.asp' Multiple SQL Injections
| asp/webapps/29[01;31m[K23[m[K1.txt

DomainSale PHP Script 1.0 - 'id' SQL Injection
| php/webapps/43[01;31m[K23[m[K5.txt

Dota 2 7.[01;31m[K23[m[Kf - Denial of Service (PoC)
| windows/dos/48031.txt

dotProject 2.0 - '/modules/public/calendar.php?baseDir' Remote File
Inclusion |
php/webapps/272[01;31m[K23[m[K.txt

dotProject 2.1.2 - Multiple SQL Injections / Cross-Site Scripting
Vulnerabilities |
php/webapps/3[01;31m[K23[m[K06.txt

douran portal 3.9.0.[01;31m[K23[m[K - Multiple Vulnerabilities
| php/webapps/8718.txt

Downstat 1.8 - 'art' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K59.txt

DPScms - 'q' SQL Injection / Cross-Site Scripting
| php/webapps/34[01;31m[K23[m[K2.txt

Dr.Web 4.x - Virus Scanner Folder Name Buffer Overflow (PoC)
| windows/dos/2[01;31m[K23[m[K28.txt

Drale DBTableViewer 1001[01;31m[K23[m[K - Blind SQL Injection
| php/webapps/39905.txt

Dreambox - Web Interface URI Remote Denial of Service
| hardware/dos/3[01;31m[K23[m[K05.txt

```
Dreamcost HostAdmin 3.0 - 'index.php' Remote File Inclusion
| php/webapps/27[01;31m[K23[m[K8.php

Drupal 10.1.2 - web-cache-poisoning-External-service-interaction
| php/webapps/517[01;31m[K23[m[K.txt

DSCounter 1.2 - 'index.php' SQL Injection
| php/webapps/274[01;31m[K23[m[K.txt

DSite CMS 4.81 - 'modmenu.php' Cross-Site Scripting
| php/webapps/343[01;31m[K23[m[K.html

dsock 1.3 - 'buf' Remote Buffer Overflow (PoC)
| multiple/dos/[01;31m[K23[m[K03.html

Dupehunter Professional 9.0.0.3911 - 'Fwpuclnt.dll' DLL Loading
Arbitrary Code Execution                    |
windows/remote/348[01;31m[K23[m[K.c

DUware Software - Multiple Vulnerabilities
| asp/webapps/[01;31m[K23[m[K561.txt

DWebPro 3.4.1 - Http.ini Plaintext Password Storage
| windows/local/[01;31m[K23[m[K037.txt

Dynamic MP3 Lister 2.0.1 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                          |
php/webapps/3[01;31m[K23[m[K64.txt

DZCP (deV!L_z Clanportal) 1.5.4 - Local File Inclusion
| php/webapps/153[01;31m[K23[m[K.txt

E Sms Script - Multiple SQL Injections
| php/webapps/[01;31m[K23[m[K967.txt

E-PHP B2B Trading Marketplace Script - 'listings.php' SQL Injection
| php/webapps/3[01;31m[K23[m[K46.txt

E107 - 'Chatbox.php' Denial of Service
| php/dos/[01;31m[K23[m[K311.txt

e107 0.7.[01;31m[K23[m[K - Multiple SQL Injections
| php/webapps/34653.txt

e107 0.7.[01;31m[K23[m[K - SQL Injection
| php/webapps/15143.txt

e107 1.0.1 - Arbitrary JavaScript Execution (via Cross-Site Request
Forgery)                                  |
php/webapps/[01;31m[K23[m[K828.txt

e107 1.0.2 - SQL Injection (via Cross-Site Request Forgery)
| php/webapps/[01;31m[K23[m[K829.txt
```

```
e107 CMS 0.7.19 - Cross-Site Request Forgery
| php/webapps/1[01;31m[K23[m[K19.txt

e107 module 1[01;31m[K23[m[K flash chat 6.8.0 - Remote File Inclusion
| php/webapps/5459.txt

e107 Plugin my_gallery 2.4.1 - 'readfile()' Local File Disclosure
| php/webapps/9[01;31m[K23[m[K5.php

EarthStation 5 - Search Service Remote File Deletion
| windows/remote/[01;31m[K23[m[K211.cpp

Easy File Sharing FTP Server 2.0 - 'PASS' Remote
| windows/remote/2[01;31m[K23[m[K4.py

Easy File Sharing Web Server 1.2 - Information Disclosure
| windows/remote/[01;31m[K23[m[K222.txt

Easy File Sharing Web Server 1.25 - Denial of Service
| windows/dos/4[01;31m[K23[m[K.pl

Easy File Sharing Web Server 7.2 - GET 'PassWD' Remote Buffer Overflow
(DEP Bypass)                          |
windows/remote/4[01;31m[K23[m[K04.py

EasyDynamicPages 1.0 - 'config_page.php' PHP Remote File Inclusion
| php/webapps/[01;31m[K23[m[K507.txt

EasyFTP Server 1.7.0.11 - 'APPE' Remote Buffer Overflow
| windows/remote/40[01;31m[K23[m[K4.py

EasyFTP Server 1.7.0.11 - (Authenticated) Multiple Commands Remote
Buffer Overflows                      |
windows/remote/146[01;31m[K23[m[K.py

EasyFTP Server 1.7.0.2 - CWD Buffer Overflow (Metasploit)
| windows/remote/1[01;31m[K23[m[K12.rb

EasyPHP - 'main.php' SQL Injection
| php/webapps/370[01;31m[K23[m[K.txt

EasyPublish CMS [01;31m[K23[m[K.04.2010 - URI Cross-Site Scripting
| php/webapps/33970.txt

Easyzip 2000 3.5 - '.zip' Local Stack Buffer Overflow
| windows/local/1[01;31m[K23[m[K79.php

eCommerce Corporation Online Store Kit 3.0 - 'listing.php?id' SQL
Injection                             |
php/webapps/[01;31m[K23[m[K720.txt
```

```
eCommerce Corporation Online Store Kit 3.0 - 'More.php' Cross-Site
Scripting                                  |
php/webapps/[01;31m[K23[m[K712.txt

eCommerce Corporation Online Store Kit 3.0 - 'More.php?id' SQL
Injection                                   |
php/webapps/[01;31m[K23[m[K711.txt

eCommerce Corporation Online Store Kit 3.0 - 'shop.php?cat' SQL
Injection                                  |
php/webapps/[01;31m[K23[m[K718.txt

eCommerce Corporation Online Store Kit 3.0 -
'shop_by_brand.php?cat_manufacturer' SQL Injection            |
php/webapps/[01;31m[K23[m[K719.txt

Edimax AR-6004 ADSL Router - Management Interface Cross-Site Scripting
| hardware/remote/[01;31m[K23[m[K528.txt

eDirectory - SQL Injection
| php/webapps/464[01;31m[K23[m[K.txt

eDonkey Clients 0.44/0.45 - Multiple Chat Dialog Resource Consumption
Vulnerabilities                        |
windows/dos/2[01;31m[K23[m[K95.txt

EDraw Flowchart ActiveX Control 2.3 - '.edd parsing' Buffer Overflow
| windows/local/1[01;31m[K23[m[K42.pl

EDraw Flowchart ActiveX Control 2.3 - 'EDImage.ocx' Remote Denial of
Service (IE)                            |
windows/dos/1[01;31m[K23[m[K41.txt

Educe ASP Search Engine 1.5.6 - 'search.asp' Cross-Site Scripting
| asp/webapps/3[01;31m[K23[m[K00.txt

EffectOffice Server 2.6 - Remote Service Buffer Overflow (PoC)
| multiple/dos/[01;31m[K23[m[K390.txt

Ektron 8.02 - XSLT Transform Remote Code Execution (Metasploit)
| windows/remote/[01;31m[K23[m[K155.rb

Elecard MPEG Player 5.7 - Local Buffer Overflow (PoC) (SEH)
| windows/dos/16[01;31m[K23[m[K7.py

elektropost episerver 3/4 - Multiple Vulnerabilities
| asp/webapps/[01;31m[K23[m[K440.txt

Elite Bulletin Board 2.1.21 - Multiple SQL Injections
| php/webapps/[01;31m[K23[m[K575.txt

eliteCMS 1.0 - 'page' SQL Injection
| php/webapps/3[01;31m[K23[m[K16.txt
```

```
EMC Cloud Tiering Appliance 10.0 - XML External Entity Arbitrary File
Read (Metasploit)                    |
multiple/webapps/326[01;31m[K23[m[K.txt

eMerge E3 1.00-06 - 'layout' Reflected Cross-Site Scripting
| hardware/webapps/476[01;31m[K23[m[K.txt

Emil 2.x - Multiple Buffer Overrun / Format String Vulnerabilities
| linux/remote/[01;31m[K23[m[K881.txt

Empire CMS 3.7 - 'checklevel.php' Remote File Inclusion
| php/webapps/2[01;31m[K23[m[K9.txt

empris r200209[01;31m[K23[m[K - 'phormationdir' Remote File Inclusion
| php/webapps/1895.txt

eMule 0.2x - AttachToAlreadyKnown Double-Free
| windows/remote/[01;31m[K23[m[K040.c

eMule 0.2x Client - OP_SERVERIDENT Heap Overflow
| windows/remote/[01;31m[K23[m[K038.c

Emumail EMU Webmail 5.2.7 - 'emumail.fcgi' Multiple Cross-Site
Scripting Vulnerabilities                    |
cgi/webapps/[01;31m[K23[m[K810.txt

Emumail EMU Webmail 5.2.7 - nit.emu Information Disclosure
| cgi/webapps/[01;31m[K23[m[K809.txt

eNdonesia 8.2/8.3 - 'Mod' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K067.txt

Endpoint Protector 4.0.4.2 - Multiple Persistent Cross-Site Scripting
Vulnerabilities                      |
php/webapps/2[01;31m[K23[m[K99.txt

Enterasys NetSight - 'nssyslogd.exe' Remote Buffer Overflow
(Metasploit)                                  |
windows/remote/[01;31m[K23[m[K887.rb

Enterpriser16 Load Balancer 7.1 - Multiple Cross-Site Scripting
Vulnerabilities                             |
hardware/webapps/[01;31m[K23[m[K499.txt

Enthrallweb eHomes - 'result.asp' Multiple SQL Injections
| asp/webapps/291[01;31m[K23[m[K.txt

EPay Enterprise 4.13 - 'cid' SQL Injection
| php/webapps/1[01;31m[K23[m[K53.txt

Epic 1.0.1/1.0.x - CTCP Nickname Server Message Buffer Overrun
| linux/remote/[01;31m[K23[m[K366.c
```

Epic Games Unreal Engine 436 - Client Unreal URL Denial of Service
| multiple/dos/222[01;31m[K23[m[K.txt

Epic Games Unreal Engine 436 - Multiple Format String Vulnerabilities
| multiple/remote/3[01;31m[K23[m[K63.txt

Epic Games Unreal Tournament Server 436.0 - Engine Remote Format String
| multiple/dos/[01;31m[K23[m[K799.txt

Erolife AjxGaleri VT - Database Disclosure
| asp/webapps/110[01;31m[K23[m[K.txt

Escapade 0.2.1 Beta Scripting Engine - 'PAGE' Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K127.txt

Escapade 0.2.1 Beta Scripting Engine - 'PAGE' Full Path Disclosure
| cgi/webapps/[01;31m[K23[m[K128.txt

EternalMart Mailing List Manager 1.32 - Remote File Inclusion
| php/webapps/[01;31m[K23[m[K218.txt

eTouch SamePage 4.4.0.0.[01;31m[K23[m[K9 - Multiple Vulnerabilities
| php/webapps/36089.txt

Ettercap 0.7.5.1 - Stack Overflow
| unix/dos/[01;31m[K23[m[K945.txt

EType EServ 2.9x - SMTP Remote Denial of Service
| windows/dos/221[01;31m[K23[m[K.pl

Eudora WorldMail 2.0 - Search Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K021.txt

Eureka Email Client - Remote Buffer Overflow
| windows/remote/10[01;31m[K23[m[K5.py

events Calendar 1.1 - Remote File Inclusion
| php/webapps/66[01;31m[K23[m[K.txt

EvolutionX - Multiple Remote Buffer Overflow Vulnerabilities
| windows/dos/[01;31m[K23[m[K681.pl

Exagate Sysguard 6001 - Cross-Site Request Forgery (Add Admin)
| php/webapps/48[01;31m[K23[m[K4.txt

Excitemedia CMS - SQL Injection
| php/webapps/1[01;31m[K23[m[K55.pl

ExifTool 12.[01;31m[K23[m[K - Arbitrary Code Execution
| linux/local/50911.py

ExoPHPDesk 1.2.1 - 'faq.php' SQL Injection
| php/webapps/3[01;31m[K23[m[K4.txt

Expinion.net Member Management System 2.1 - 'error.asp?err' Cross-Site Scripting |
asp/webapps/[01;31m[K23[m[K853.txt

Expinion.net Member Management System 2.1 - 'news_view.asp?ID' SQL Injection |
asp/webapps/[01;31m[K23[m[K851.txt

Expinion.net Member Management System 2.1 - 'register.asp?err' Cross-Site Scripting |
asp/webapps/[01;31m[K23[m[K854.txt

Expinion.net Member Management System 2.1 - 'resend.asp?ID' SQL Injection |
asp/webapps/[01;31m[K23[m[K852.txt

Expinion.net News Manager Lite 2.5 - 'category_news.asp?ID' SQL Injection |
asp/webapps/[01;31m[K23[m[K861.txt

Expinion.net News Manager Lite 2.5 - 'category_news_headline.asp' Cross-Site Scripting |
asp/webapps/[01;31m[K23[m[K859.txt

Expinion.net News Manager Lite 2.5 - 'comment_add.asp' Cross-Site Scripting |
asp/webapps/[01;31m[K23[m[K857.txt

Expinion.net News Manager Lite 2.5 - 'more.asp?ID' SQL Injection
| asp/webapps/[01;31m[K23[m[K860.txt

Expinion.net News Manager Lite 2.5 - 'NEWS_LOGIN?admin' Cookie Authentication Bypass |
asp/webapps/[01;31m[K23[m[K863.txt

Expinion.net News Manager Lite 2.5 - 'news_sort.asp?filter' SQL Injection |
asp/webapps/[01;31m[K23[m[K862.txt

Expinion.net News Manager Lite 2.5 - 'search.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K23[m[K858.txt

Exponent CMS 0.96.3 - 'view' Remote Command Execution
| php/webapps/[01;31m[K23[m[K91.php

Exponent CMS 2.0 Beta 1.1 - Cross-Site Request Forgery (Add Administrator Account) |
php/webapps/17[01;31m[K23[m[K5.html

Extcalendar 2 - 'profile.php' Remote User Pass Change
| php/webapps/3[01;31m[K23[m[K9.html

```
extent technologies rbs isp 2.5 - Directory Traversal
| multiple/remote/20[01;31m[K23[m[K4.txt

eXtrovert software Thyme 1.3 - 'add_calendars.php' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K98.txt

eXtrovert software Thyme 1.3 - 'pick_users.php' SQL Injection
| php/webapps/3[01;31m[K23[m[K42.txt

EzASPSite 2.0 RC3 - 'Scheme' SQL Injection
| asp/webapps/16[01;31m[K23[m[K.pl

Ezboard - 'invitefriends.php3' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K072.txt

EZBoard 7.3 - Font Tag HTML Injection
| php/webapps/[01;31m[K23[m[K744.txt

EZMeeting 3.x - 'EZNet.exe' Long HTTP Request Remote Buffer Overflow
| windows/remote/[01;31m[K23[m[K417.pl

EZPhotoShare 1.0/1.1 - Memory Corruption
| windows/dos/[01;31m[K23[m[K412.pl

F-Secure BackWeb 6.31 - Local Privilege Escalation
| windows/local/[01;31m[K23[m[K910.txt

F5 Networks BIG-IP - XML External Entity Injection
| hardware/remote/38[01;31m[K23[m[K3.txt

Facebook Profile MyBB Plugin 2.4 - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K355.txt

Facil-CMS 0.1RC2 - Multiple Vulnerabilities
| php/webapps/8[01;31m[K23[m[K7.txt

Fake Hit Generator 2.2 - Arbitrary File Upload
| php/webapps/10[01;31m[K23[m[K0.txt

Family CMS 2.7.2 - Multiple Persistent Cross-Site Scripting
Vulnerabilities                                 |
php/webapps/18[01;31m[K23[m[K0.txt

Fastream NetFile 6.0.3.588 - Error Message Cross-Site Scripting
| multiple/remote/[01;31m[K23[m[K307.txt

FCKEditor Core ASP 2.6.8 - Arbitrary File Upload Protection Bypass
| asp/webapps/[01;31m[K23[m[K005.txt

FCMS CMS 2.7.2 - Multiple Cross-Site Request Forgery Vulnerabilities
| php/webapps/18[01;31m[K23[m[K2.txt
```

```
FdWeB Espace Membre 2.01 - 'path' Remote File Inclusion
| php/webapps/31[01;31m[K23[m[K.html

FFmpeg 0.5 - Multiple Remote Vulnerabilities
| linux/dos/33[01;31m[K23[m[K3.txt

File 3.x - Local Stack Overflow Code Execution (1)
| unix/local/2[01;31m[K23[m[K24.c

File 3.x - Local Stack Overflow Code Execution (2)
| unix/local/2[01;31m[K23[m[K25.c

File 3.x - Utility Local Memory Allocation
| linux/local/2[01;31m[K23[m[K26.c

file sharing for net 1.5 - Directory Traversal
| windows/remote/[01;31m[K23[m[K068.txt

Finjan SurfinGate 6.0/7.0 - FHTTP Restart Command Execution
| linux/remote/[01;31m[K23[m[K585.txt

Fire Soft Board RC 3 - 'racine' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K19.txt

FireFly Mediaserver 1.0.0.1359 - Null Pointer Dereference
| windows/dos/[01;31m[K23[m[K574.txt

Firefox 50.0.1 - ASM.JS JIT-Spray Remote Code Execution
| windows/remote/4[01;31m[K23[m[K27.html

Firefox 54.0.1 - Denial of Service
| windows/dos/4[01;31m[K23[m[K02.txt

FirePass SSL VPN - Local File Inclusion
| multiple/webapps/[01;31m[K23[m[K111.txt

Flashden - Multiple Arbitrary File Uploads
| php/webapps/10[01;31m[K23[m[K6.txt

Flatnux 2010-06.09 - 'find' Cross-Site Scripting
| php/webapps/34[01;31m[K23[m[K4.txt

FloosieTek FTGate 2.1 - Web File Access
| multiple/remote/192[01;31m[K23[m[K.txt

FloosieTek FTGate Mail Server 1.2 - 'index.fts?folder' Cross-Site
Scripting                                  |
cgi/webapps/[01;31m[K23[m[K913.txt

FloosieTek FTGate Mail Server 1.2 - Full Path Disclosure
| cgi/webapps/[01;31m[K23[m[K914.txt
```

FloosieTek FTGatePro 1.2 - WebAdmin Interface Information Disclosure
| windows/remote/[01;31m[K23[m[K135.txt

FloosieTek FTGatePro 1.22 - Mail Server Cross-Site Scripting
| windows/remote/[01;31m[K23[m[K092.txt

FloosieTek FTGatePro 1.22 - Mail Server Full Path Disclosure
| windows/remote/[01;31m[K23[m[K091.txt

Flying Dog Software Powerslave 4.3 Portalmanager - 'sql_id' Information
Disclosure | php/webapps/[01;31m[K23[m[K163.txt

Fonality trixbox - SQL Injection
| php/webapps/32[01;31m[K23[m[K9.txt

Fool's Workshop Owl's Workshop 1.0 - '/glossaries/index.php?File'
Arbitrary File Access |
php/webapps/[01;31m[K23[m[K725.txt

Fool's Workshop Owl's Workshop 1.0 - 'glossary.php' Arbitrary File
Access |
php/webapps/[01;31m[K23[m[K7[01;31m[K23[m[K.txt

Fool's Workshop Owl's Workshop 1.0 - 'multiplechoice/index.php'
Arbitrary File Access |
php/webapps/[01;31m[K23[m[K722.txt

Fool's Workshop Owl's Workshop 1.0 - 'newmultiplechoice.php' Arbitrary
File Access |
php/webapps/[01;31m[K23[m[K724.txt

Fool's Workshop Owl's Workshop 1.0 - 'readings/index.php' Arbitrary
File Access |
php/webapps/[01;31m[K23[m[K726.txt

Fool's Workshop Owl's Workshop 1.0 - 'resultsignore.php' Arbitrary File
Access | php/webapps/[01;31m[K23[m[K727.txt

Fortigate Firewall 2.x - dlg Admin Interface Cross-Site Scripting
| hardware/remote/[01;31m[K23[m[K376.txt

Fortigate Firewall 2.x - listdel Admin Interface Cross-Site Scripting
| hardware/remote/[01;31m[K23[m[K378.txt

Fortigate Firewall 2.x - Policy Admin Interface Cross-Site Scripting
| hardware/remote/[01;31m[K23[m[K377.txt

Fortigate Firewall 2.x - selector Admin Interface Cross-Site Scripting
| hardware/remote/[01;31m[K23[m[K379.txt

Fortinet FortiOS < 5.6.0 - Cross-Site Scripting
| hardware/webapps/4[01;31m[K23[m[K88.txt

```
Fortinet FortiOS_ FortiProxy_ and FortiSwitchManager 7.2.0 -
Authentication bypass                          |
windows/remote/52[01;31m[K23[m[K9.py

Fortra GoAnywhere MFT 7.4.1 - Authentication Bypass
| multiple/remote/5[01;31m[K23[m[K08.py

Foswiki MAKETEXT - Remote Command Execution (Metasploit)
| unix/remote/[01;31m[K23[m[K580.rb

Foxit Reader 5.4.4.1128 Firefox Plugin - 'npFoxitReaderPlugin.dll'
Stack Buffer Overflow (PoC)             |
windows/dos/[01;31m[K23[m[K944.php

Foxit WAC Remote Access Server 2.0 Build 3503 - Heap Buffer Overflow
| multiple/dos/31[01;31m[K23[m[K2.txt

FoxPlayer 2.9.0 - Denial of Service
| windows/dos/[01;31m[K23[m[K9[01;31m[K23[m[K.py

FoxWeb 2.5 - PATH_INFO Remote Buffer Overrun
| windows/dos/[01;31m[K23[m[K102.pl

Free Blog 1.0 - Multiple Vulnerabilities
| php/webapps/[01;31m[K23[m[K994.txt

Free Download Manager - Stack Buffer Overflow
| windows/dos/3[01;31m[K23[m[K32.txt

Free Hosting Manager 2.0 - 'id' SQL Injection
| php/webapps/[01;31m[K23[m[K028.txt

Free Opener - Local Denial of Service
| windows/dos/182[01;31m[K23[m[K.pl

FreeBSD 4.10/5.x - 'execve()' Unaligned Memory Access Denial of Service
| freebsd/dos/24[01;31m[K23[m[K3.c

Freefloat FTP Server - 'PUT' Remote Buffer Overflow
| windows/remote/2[01;31m[K23[m[K51.py

Freefloat FTP Server - 'USER' Remote Buffer Overflow
| windows/remote/[01;31m[K23[m[K243.py

Freefloat FTP Server - Arbitrary File Upload (Metasploit)
| windows/remote/[01;31m[K23[m[K226.rb

Freefloat FTP Server 1.0 - Remote Buffer Overflow
| multiple/remote/5[01;31m[K23[m[K[01;31m[K23[m[K.txt

Freeform Interactive Purge 1.4.7/Purge Jihad 2.0.1 Game Client - Remote
Buffer Overflow                    |
multiple/remote/[01;31m[K23[m[K707.txt
```

freeFTPd 1.2.6 - Remote Authentication Bypass
| windows/remote/[01;31m[K23[m[K079.txt

FreePBX 13/14 - Remote Command Execution / Privilege Escalation
| linux/remote/40[01;31m[K23[m[K2.py

FreeRadius 0.x/1.1.x - Tag Field Heap Corruption
| linux/dos/[01;31m[K23[m[K391.txt

freeSSHd 2.1.3 - Remote Authentication Bypass
| windows/remote/[01;31m[K23[m[K080.txt

FreeVimager 4.1.0 - Crash (PoC)
| windows/dos/[01;31m[K23[m[K280.py

Freewebscriptz Online Games Login - Multiple SQL Injections
| windows/remote/34[01;31m[K23[m[K0.txt

Fresh Guest Book 1.0/2.x - HTML Injection
| cgi/webapps/[01;31m[K23[m[K890.txt

FreznoShop 1.2.3/1.3 - Search Script Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K519.txt

Friendly Technologies - 'fwRemoteCfg.dll' ActiveX Remote Buffer
Overflow |
windows/remote/63[01;31m[K23[m[K.html

Friends in War Make or Break 1.7 - Authentication Bypass
| php/webapps/4[01;31m[K23[m[K79.txt

Friends in War Make or Break 1.7 - Cross-Site Request Forgery (Change
Admin Password) |
php/webapps/4[01;31m[K23[m[K83.html

Friends in War Make or Break 1.7 - SQL Injection
| php/webapps/4[01;31m[K23[m[K81.txt

Front Accounting 2.3.4 - Cross-Site Request Forgery
| php/webapps/17[01;31m[K23[m[K8.html

FTP Desktop 3.5 - Banner Parsing Buffer Overflow
| windows/dos/[01;31m[K23[m[K117.txt

FTP Desktop 3.5 - FTP 331 Server Response Buffer Overflow
| windows/dos/[01;31m[K23[m[K118.txt

FTPGetter 5.89.0.85 - Remote Buffer Overflow (SEH)
| windows/remote/4[01;31m[K23[m[K28.py

FTPGetter Professional 5.97.0.2[01;31m[K23[m[K - Denial of Service
(PoC) |
windows/dos/47871.txt

Fuel CMS 1.4.13 - 'col' Blind SQL Injection (Authenticated)
| php/webapps/505[01;31m[K23[m[K.txt

Full PHP Emlak Script - 'landsee.php' SQL Injection
| php/webapps/3[01;31m[K23[m[K09.txt

Fullaspsite Asp Hosting Sitesi - 'tr' SQL Injection
| asp/webapps/3[01;31m[K23[m[K3.txt

Fusion News 3.3 - Unauthorized Account Addition
| php/webapps/[01;31m[K23[m[K039.txt

FusionInvoice 20[01;31m[K23[m[K-1.0 - Stored XSS (Cross-Site Scripting)
| multiple/webapps/51480.txt

futurewave webx server 1.1 - Directory Traversal
| multiple/remote/[01;31m[K23[m[K136.txt

Fuzzylime CMS 3.03 - 'track.php' Local File Inclusion
| php/webapps/7[01;31m[K23[m[K1.txt

FuzzyMonkey 2.11 - MyClassifieds Email Variable SQL Injection
| php/webapps/[01;31m[K23[m[K269.txt

FVWM 2.4.17/2.5.8 - fvwm_make_browse_menu.sh Scripts Command Execution
| linux/local/[01;31m[K23[m[K849.txt

FVWM 2.4/2.5 - fvwm-menu-Directory Command Execution
| linux/local/[01;31m[K23[m[K414.txt

G-WAN 2.10.6 - Buffer Overflow (Denial of Service) (PoC)
| multiple/dos/36[01;31m[K23[m[K4.txt

G5 Scripts Guestbook PHP 1.2.8 - Cross-Site Scripting
| php/webapps/1[01;31m[K23[m[K74.txt

Galerie Dezign-Box France - Multiple Vulnerabilities
| php/webapps/115[01;31m[K23[m[K.txt

Gallery 1.3.x/1.4 - Remote Global Variable Injection
| php/webapps/[01;31m[K23[m[K599.txt

Gallery 1.4 - 'index.php' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K[01;31m[K23[m[K8.txt

Gallery 2.0 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K23[m[K40.txt

Gamespy 3d 2.62/2.63 - IRC Client Remote Buffer Overflow
| linux/dos/[01;31m[K23[m[K200.txt

Gamespy Software Development Kit - Remote Denial of Service
| linux/dos/[01;31m[K23[m[K757.txt

Garage Management System 1.0 (categoriesName) - Stored XSS
| multiple/webapps/52[01;31m[K23[m[K8.txt

Garbage Collection Management System 1.0 - SQL Injection + Arbitrary File Upload |
php/webapps/501[01;31m[K23[m[K.py

Gauntlet Firewall for Unix 6.0 - SQL-GW Connection Denial of Service
| linux/dos/[01;31m[K23[m[K172.txt

GDAM1[01;31m[K23[m[K 0.933/0.942 - Filename Buffer Overflow
| unix/local/21760.c

gdb (GNU debugger) 7.5.1 - Null Pointer Dereference
| linux/dos/[01;31m[K23[m[K5[01;31m[K23[m[K.c

GEdit 2.0/2.2 - Large IOStream File Memory Corruption
| linux/dos/[01;31m[K23[m[K393.c

geeeekShop 1.4 - Information Disclosure
| php/webapps/[01;31m[K23[m[K000.txt

Geeklog 1.3.8 - Forgot Password SQL Injection
| php/webapps/[01;31m[K23[m[K260.sh

Geeklog 1.3.x - Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K194.txt

GeekLog 1.3.x - HTML Injection
| php/webapps/[01;31m[K23[m[K[01;31m[K23[m[K3.txt

Geeklog 1.3.x - SQL Injection
| php/webapps/[01;31m[K23[m[K193.txt

gelato CMS 0.95 - 'img' Remote File Disclosure
| php/webapps/6[01;31m[K23[m[K5.txt

Gene6 BPFTP FTP Server 2.0 - User Credentials Disclosure
| windows/remote/207[01;31m[K23[m[K.pl

GenPortal - 'buscarCat.php' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K08.txt

Gentoo-Specific MPG1[01;31m[K23[m[K - URI Remote Buffer Overflow
| linux/dos/28160.txt

GetWare Web Server Component - Content-Length Value Remote Denial of Service |
multiple/dos/[01;31m[K23[m[K556.txt

GFI Faxmaker Fax Viewer 10.0 (build [01;31m[K23[m[K7) - Denial of Service (PoC) |
windows/dos/18043.py

```
Ghidra (Linux) 9.0.4 - .gar Arbitrary Code Execution
| linux/local/47[01;31m[K23[m[K1.py

GitBucket 4.[01;31m[K23[m[K.1 - Remote Code Execution
| java/webapps/44668.py

GitHub Enterprise < 2.8.7 - Remote Code Execution
| multiple/webapps/4[01;31m[K23[m[K92.py

GitLab - 'impersonate' Feature Privilege Escalation
| ruby/webapps/40[01;31m[K23[m[K6.txt

GL.iNet AR300M v3.216 Remote Code Execution - CVE-20[01;31m[K23[m[K-
46456 Exploit                                          |
hardware/remote/51854.py

GL.iNet AR300M v4.3.7 Arbitrary File Read - CVE-20[01;31m[K23[m[K-46455
Exploit                                              |
hardware/remote/51851.py

GL.iNet AR300M v4.3.7 Remote Code Execution - CVE-20[01;31m[K23[m[K-
46454 Exploit                                          |
hardware/remote/51852.py

GlassFish Application Server - '/resourceNode/externalResourceNew.jsf'
Multiple Cross-Site Scripting Vulne |
multiple/remote/319[01;31m[K23[m[K.txt

GlobalScape Secure FTP Server 2.0 Build 03.11.2004.2 - Site Command
Remote Buffer Overflow                 |
windows/dos/[01;31m[K23[m[K839.pl

GLPI  Cartography Plugin v6.0.0 - Unauthenticated Remote Code Execution
(RCE)                                | php/webapps/51[01;31m[K23[m[K4.txt

GLPI Activity  v3.1.0 - Authenticated Local File Inclusion on Activity
plugin                                |
php/webapps/51[01;31m[K23[m[K2.txt

GLPI Glpiinventory v1.0.1 - Unauthenticated Local File Inclusion
| php/webapps/51[01;31m[K23[m[K0.txt

GLPI v10.0.2 - SQL Injection (Authentication Depends on Configuration)
| php/webapps/51[01;31m[K23[m[K3.txt

Gnome 1.0/1.1 / Group X 11.0 / XFree86 X11R6 3.3.x/4.0 - Denial of
Service                                  |
linux/dos/200[01;31m[K23[m[K.c

GNOME Eye Of Gnome 1.0.x/1.1.x/2.2 - Format String
| linux/local/2[01;31m[K23[m[K76.txt
```

GNU Anubis 3.6.x/3.9.x - 'auth.c auth_ident()' Remote Overflow
| linux/remote/[01;31m[K23[m[K772.c

GNU Anubis 3.6.x/3.9.x - Multiple Format String Vulnerabilities
| linux/remote/[01;31m[K23[m[K771.pl

GNU CFEngine 2.0.x - CFServD Transaction Packet Buffer Overrun (1)
| linux/remote/[01;31m[K23[m[K182.c

GNU CFEngine 2.0.x - CFServD Transaction Packet Buffer Overrun (2)
| linux/remote/[01;31m[K23[m[K183.c

GNU Coreutils 'sort' Text Utility - Local Buffer Overflow
| linux/local/38[01;31m[K23[m[K2.txt

GNU glibc 2.x - 'strfmon()' Integer Overflow
| linux/dos/33[01;31m[K23[m[K0.txt

GNU Indent 2.2.9 - Local Heap Overflow
| linux/local/[01;31m[K23[m[K479.sh

GNU libiberty - Buffer Overflow
| linux/dos/4[01;31m[K23[m[K86.txt

GNU Mailutils imap4d 0.6 (FreeBSD) - 'Search' Remote Format String
| bsd/remote/1[01;31m[K23[m[K4.c

GNU Mailutils imap4d 0.6 - Remote Format String
| linux/remote/11[01;31m[K23[m[K.c

GNU Make For IBM AIX 4.3.3 - CC Path Local Buffer Overflow
| aix/local/[01;31m[K23[m[K838.pl

GNU MyProxy 20030629 - Cross-Site Scripting
| linux/remote/[01;31m[K23[m[K801.txt

GNU Zebra 0.9x / Quagga 0.96 - Remote Denial of Service
| linux/dos/[01;31m[K23[m[K375.txt

GnuPG 1.x - Detached Signature Verification Bypass
| linux/local/27[01;31m[K23[m[K1.txt

GNUTURK 2G - 't_id' SQL Injection
| php/webapps/[01;31m[K23[m[K78.php

GoAhead Web Server 2.1.x - '.ASP' File Source Code Disclosure
| windows/remote/[01;31m[K23[m[K446.txt

GoAhead Web Server 2.1.x - Directory Management Policy Bypass
| windows/remote/[01;31m[K23[m[K555.txt

GOautodial 4.0 - Authenticated Shell Upload
| php/webapps/489[01;31m[K23[m[K.txt

```
GoAutoDial CE 2.0 - Arbitrary File Upload
| php/webapps/36[01;31m[K23[m[K1.py

Gogs - 'label' SQL Injection
| multiple/webapps/35[01;31m[K23[m[K7.txt

Gogs - 'users'/'repos' '?q' SQL Injection
| multiple/webapps/35[01;31m[K23[m[K8.txt

Gold MP4 Player 3.3 - Universal (SEH) (Metasploit)
| windows/dos/3[01;31m[K23[m[K29.rb

GoldLink 3.0 - Cookie SQL Injection
| php/webapps/[01;31m[K23[m[K259.txt

GoldWave 5.70 - Local Buffer Overflow (SEH Unicode)
| windows/local/444[01;31m[K23[m[K.py

Gom Player 2.1.44.51[01;31m[K23[m[K - 'UNICODE' Null Pointer
Dereference                                                 |
windows/dos/21830.py

GoodTech Telnet Server 4.0 - Remote Denial of Service
| windows/dos/[01;31m[K23[m[K506.txt

Google AD Sync Tool - Exposure of Sensitive Information
| multiple/local/249[01;31m[K23[m[K.txt

Google Android - 'rkp_set_init_page_ro' RKP Memory Corruption
| android/dos/41[01;31m[K23[m[K2.txt

Google Android 2.0 < 2.1 - Code Execution (Reverse Shell
10.0.2.2:2222/TCP)                                  |
android/remote/154[01;31m[K23[m[K.html

Google Android Kernel 2.6 - Local Denial of Service Crash (PoC)
| android/dos/[01;31m[K23[m[K248.txt

Google Chrome 0.2.149 - Malformed 'title' Tag Remote Denial of Service
| multiple/dos/3[01;31m[K23[m[K11.html

Google Chrome 0.2.149 - Malformed 'view-source' HTTP Header Remote
Denial of Service                        |
multiple/dos/3[01;31m[K23[m[K35.js

Google Chrome 2.0.172 - 'About:blank' Address Bar URI Spoofing
'About:blank' Address Bar URI Spoofing      |
multiple/remote/331[01;31m[K23[m[K.html

Google Chrome 8.0.552.[01;31m[K23[m[K7 - address Overflow Denial of
Service                                                  |
windows/dos/16012.html
```

Google Chrome 8.0.552.[01;31m[K23[m[K7 - replace Denial of Service
| multiple/dos/16079.html

Google Chrome 80.0.3987.87 - Heap-Corruption Remote Denial of Service
(PoC) |
windows/dos/48[01;31m[K23[m[K7.txt

Google Desktop - Cross-Site Scripting
| cgi/webapps/296[01;31m[K23[m[K.txt

Google Hack Honeypot File Upload Manager 1.3 - 'delall' Unauthorized
File Access |
php/webapps/31[01;31m[K23[m[K9.txt

Gordano Messaging Suite 9.0 - 'WWW.exe' Denial of Service
| windows/dos/[01;31m[K23[m[K130.txt

Gordano NTMail 3.0/5.0 - SPAM Relay
| aix/remote/19[01;31m[K23[m[K7.txt

gpEasy CMS - 'section' Cross-Site Scripting
| php/webapps/38[01;31m[K23[m[K6.txt

Grand Theft Auto III/Vice City Skin File v1.1 - Buffer Overflow
| windows/local/512[01;31m[K23[m[K.py

Grandstream GSD3710 1.0.11.13 - Stack Buffer Overflow
| multiple/remote/5[01;31m[K23[m[K03.py

Grandstream GSD3710 1.0.11.13 - Stack Overflow
| multiple/remote/5[01;31m[K23[m[K13.py

GrapAgenda 0.1 - 'page' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K04.txt

Grep < 2.11 - Integer Overflow Crash (PoC)
| linux/dos/[01;31m[K23[m[K779.txt

Groone's GLink ORGanizer 2.1 - 'cat' Blind SQL Injection
| php/webapps/9[01;31m[K23[m[K6.txt

GTCatalog 0.8.16/0.9 - Remote File Inclusion
| php/webapps/2[01;31m[K23[m[K17.txt

guanxiCRM Business Solution 0.9.1 - Remote File Inclusion
| php/webapps/[01;31m[K23[m[K81.txt

GuppY 2.4 - Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K219.txt

GuppY 2.4 - HTML Injection
| php/webapps/[01;31m[K23[m[K192.txt

```
GuppY 2.4 - Remote File Access
| php/webapps/[01;31m[K23[m[K220.txt

Guru Auction 2.0 - Multiple SQL Injections
| php/webapps/[01;31m[K23[m[K673.txt

GWeb HTTP Server 0.5/0.6 - Directory Traversal
| windows/remote/[01;31m[K23[m[K758.txt

Haberx 1.02 < 1.1 - 'tr' SQL Injection
| asp/webapps/[01;31m[K23[m[K71.txt

Hailboards 1.2.0 - 'phpbb_root_path' Remote File Inclusion
| php/webapps/3[01;31m[K23[m[K6.txt

Half-Life 1.1 - Invalid Command Error Response Format String
| windows/remote/[01;31m[K23[m[K198.txt

Hand-Crafted Software FreeProxy 3.5/3.6 - FreeWeb CreateFile Function
Denial of Service                    |
windows/dos/[01;31m[K23[m[K534.txt

Hand-Crafted Software FreeProxy 3.5/3.6 - FreeWeb Directory Traversal
| windows/remote/[01;31m[K23[m[K532.txt

haneWIN DNS Server 1.5.3 - Remote Buffer Overflow (Metasploit)
| windows/remote/427[01;31m[K23[m[K.rb

Hashicorp vagrant-vmware-fusion 4.0.[01;31m[K23[m[K - Local Privilege
Escalation                                           |
macos/local/43224.sh

Hashicorp vagrant-vmware-fusion 4.0.24 - Local Privilege Escalation
| macos/local/432[01;31m[K23[m[K.sh

Hashicorp vagrant-vmware-fusion < 4.0.20 - Local Privilege Escalation
| macos/local/4[01;31m[K23[m[K34.txt

Hassan Consulting Shopping Cart 1.[01;31m[K23[m[K - Arbitrary Command
Execution                                            | cgi/remote/21104.pl

HD Soft Windows FTP Server 1.5/1.6 - 'Username' Format String
| windows/remote/[01;31m[K23[m[K531.c

Heatmiser Netmonitor 3.03 - Hardcoded Credentials
| hardware/webapps/478[01;31m[K23[m[K.txt

Heatmiser Wifi Thermostat 1.7 - Credential Disclosure
| hardware/webapps/456[01;31m[K23[m[K.sh

Herberlin BremsServer 1.2.4 - Cross-Site Scripting
| multiple/remote/[01;31m[K23[m[K600.txt
```

```
herberlin bremsserver 1.2.4/3.0 - Directory Traversal
| windows/remote/[01;31m[K23[m[K603.py

Hex Workshop 4.[01;31m[K23[m[K/5.1/6.0 - '.hex' Universal Local Buffer
Overflow (SEH)                                    |
windows/local/9550.py

Hikvision IP Camera 5.4.0 - User Enumeration (Metasploit)
| hardware/webapps/45[01;31m[K23[m[K1.rb

hMAilServer 5.3.3 - IMAP Remote Crash (PoC)
| windows/dos/2[01;31m[K23[m[K02.rb

HolaCMS 1.2.x - 'HTMLtags.php' Local File Inclusion
| php/webapps/[01;31m[K23[m[K027.txt

Homematic CCU2 2.29.[01;31m[K23[m[K - Arbitrary File Write
| cgi/webapps/44361.rb

Homematic CCU2 2.29.[01;31m[K23[m[K - Remote Command Execution
| cgi/webapps/44368.rb

Horde 3.2 - MIME Attachment Filename Insufficient Filtering Cross-Site
Scripting                            |
php/webapps/3[01;31m[K23[m[K54.txt

Horde Application Framework 3.2.1 - Forward Slash Insufficient
Filtering Cross-Site Scripting              |
php/webapps/3[01;31m[K23[m[K53.txt

Horizon Web Builder - 'fshow.php' SQL Injection
| php/webapps/17[01;31m[K23[m[K7.txt

HostAdmin - Full Path Disclosure
| php/webapps/[01;31m[K23[m[K020.txt

Hot Links SQL-PHP - 'news.php' SQL Injection
| php/webapps/3[01;31m[K23[m[K55.txt

HotNews 0.x - 'config[incdir]' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K518.txt

HotNews 0.x - 'hotnews-engine.inc.php3?config[header]' Remote File
Inclusion                                  |
php/webapps/[01;31m[K23[m[K517.txt

HP Data Protector - DtbClsLogin Buffer Overflow (Metasploit)
| windows/remote/[01;31m[K23[m[K290.rb

HP Diagnostics Server - 'magentservice.exe' Remote Overflow
(Metasploit)                                      |
windows/remote/184[01;31m[K23[m[K.rb
```

HP Digital Imaging - 'hpodio08.dll' Insecure Method
| windows/remote/1[01;31m[K23[m[K67.html

HP JetDirect Printer - SNMP JetAdmin Device Password Disclosure
| hardware/remote/2[01;31m[K23[m[K19.txt

HP OpenView Network Node Manager 6.10 - SNMP Denial of Service
| multiple/dos/20[01;31m[K23[m[K9.txt

HP Operations Agent - Opcode 'coda.exe' 0x34 Buffer Overflow
(Metasploit) |
windows/remote/2[01;31m[K23[m[K06.rb

HP Operations Agent - Opcode 'coda.exe' 0x8c Buffer Overflow
(Metasploit) |
windows/remote/2[01;31m[K23[m[K05.rb

HP Operations Manager 8.16 - 'srcvw4.dll' 'LoadFile()'/'SaveFile()'
Remote Unicode Stack Overflow (PoC) |
windows/dos/1[01;31m[K23[m[K02.html

HP Web Jetadmin 7.5.2456 - Arbitrary Command Execution
| windows/remote/[01;31m[K23[m[K880.txt

HP Web Jetadmin 7.5.2456 - Printer Firmware Update Script Arbitrary
File Upload |
windows/remote/[01;31m[K23[m[K878.txt

HP Web Jetadmin 7.5.2456 - setinfo.hts Script Directory Traversal
| windows/remote/[01;31m[K23[m[K879.txt

HP-UX 10/11 - NLSPATH Environment Variable Format String (1)
| hp-ux/local/[01;31m[K23[m[K341.c

HP-UX 10/11 - NLSPATH Environment Variable Format String (2)
| hp-ux/local/[01;31m[K23[m[K342.c

HP-UX 11 - Software Distributor Lang Environment Variable Local Buffer
Overrun | hp-ux/local/[01;31m[K23[m[K343.c

HP-UX 11 CDE DTPrintInfo - Display Environment Variable Buffer Overflow
| hp-ux/dos/[01;31m[K23[m[K[01;31m[K23[m[K6.txt

HPUX 10.20/11 Wall Message - Local Buffer Overflow
| hp-ux/local/22[01;31m[K23[m[K1.txt

HTML Help Workshop 4.74 - hhp Universal Buffer Overflow
| windows/local/103[01;31m[K23[m[K.py

HTML::BBCode 1.03/1.04 - HTML Injection
| php/webapps/27[01;31m[K23[m[K7.txt

```
htmlLawed 1.2.5 - Remote Code Execution (RCE)
| php/webapps/520[01;31m[K23[m[K.sh

http commander 4.0 - Directory Traversal
| asp/webapps/[01;31m[K23[m[K326.txt

Huawei HG255 - Directory Traversal (Metasploit)
| hardware/webapps/479[01;31m[K23[m[K.rb

Huawei Technologies eSpace Meeting Service 1.0.0.[01;31m[K23[m[K -
Local Privilege Escalation                              |
windows/local/32205.txt

Hudson 1.2[01;31m[K23[m[K - 'q' Cross-Site Scripting
| php/webapps/32047.txt

Hylafax 4.1.x - HFaxD Format String
| linux/remote/[01;31m[K23[m[K371.c

Hyperoptic (Tilgin) Router HG[01;31m[K23[m[Kxx - Multiple
Vulnerabilities                                                 |
hardware/webapps/39951.txt

HyperStop WebHost Directory 1.2 - Database Disclosure
| php/webapps/3[01;31m[K23[m[K95.txt

IA WebMail Server 3.0/3.1 - GET Buffer Overrun
| windows/remote/[01;31m[K23[m[K334.pl

IBM AIX 5.3 SP6 - 'pioout' Arbitrary Library Loading Privilege
Escalation                                      |
aix/local/4[01;31m[K23[m[K2.sh

IBM AIX 5.3 SP6 - Capture Terminal Sequence Privilege Escalation
| aix/local/4[01;31m[K23[m[K1.c

IBM AIX 5.3 SP6 - FTP 'gets()' Local Privilege Escalation
| aix/local/4[01;31m[K23[m[K3.c

IBM Bladecenter Management - Multiple Web Application Vulnerabilities
| php/webapps/14[01;31m[K23[m[K7.txt

IBM Business Process Manager - User Account Reconfiguration
| windows/webapps/314[01;31m[K23[m[K.txt

IBM Cognos - 'tm1admsd.exe' Remote Overflow (Metasploit)
| windows/remote/[01;31m[K23[m[K969.rb

IBM DB2 - 'db2govd' Command Line Argument Local Overflow
| linux/dos/[01;31m[K23[m[K349.txt

IBM DB2 - 'db2govd' Format String Arbitrary Code Execution
| linux/local/[01;31m[K23[m[K346.txt
```

IBM DB2 - 'db2start' Command Line Argument Local Overflow
| linux/dos/[01;31m[K23[m[K347.txt

IBM DB2 - 'db2start' Format String Arbitrary Code Execution
| linux/local/[01;31m[K23[m[K344.txt

IBM DB2 - 'db2stop' Command Line Argument Local Overflow
| linux/dos/[01;31m[K23[m[K348.txt

IBM DB2 - 'db2stop' Format String Arbitrary Code Execution
| linux/local/[01;31m[K23[m[K345.txt

IBM DB2 db2dart - Buffer Overflow
| linux/dos/[01;31m[K23[m[K112.txt

IBM Director < 5.10 - 'Redirect.bat' Directory Traversal
| windows/remote/[01;31m[K23[m[K20.txt

IBM Directory Server 4.1 - Web Administration Interface Cross-Site
Scripting | cgi/webapps/[01;31m[K23[m[K410.txt

IBM Informix Dynamic Server 9.40/Informix Extended Parallel Server 8.40
- Multiple Vulnerabilities (1) | unix/local/[01;31m[K23[m[K609.sh

IBM Informix Dynamic Server 9.40/Informix Extended Parallel Server 8.40
- Multiple Vulnerabilities (2) | unix/local/[01;31m[K23[m[K610.c

IBM Lotus Domino 6.5.1 - HTTP webadmin.nsf Quick Console Cross-Site
Scripting | windows/remote/[01;31m[K23[m[K837.txt

IBM Lotus Domino 6/7 - HTTP webadmin.nsf Directory Traversal
| windows/remote/[01;31m[K23[m[K836.txt

IBM Lotus iNotes dwa85W - ActiveX Buffer Overflow (Metasploit)
| windows/remote/[01;31m[K23[m[K736.rb

IBM Lotus Notes Client URL Handler - Command Injection (Metasploit)
| windows/remote/[01;31m[K23[m[K650.rb

IBM Lotus QuickR qp2 - ActiveX Buffer Overflow (Metasploit)
| windows/remote/[01;31m[K23[m[K737.rb

IBM Net.Data 7.0/7.2 - db2www Error Message Cross-Site Scripting
| multiple/remote/[01;31m[K23[m[K598.txt

IBM Security Verify Access 10.0.0 - Open Redirect during OAuth Flow
| multiple/webapps/521[01;31m[K23[m[K.NA

IBM System Director Agent - DLL Injection (Metasploit)
| windows/remote/[01;31m[K23[m[K203.rb

```
IBM System Director Agent - Remote System Level
| windows/remote/[01;31m[K23[m[K074.txt

Icarus 2.0 - '.pgn' Local Stack Overflow (SEH)
| windows/local/8[01;31m[K23[m[K6.py

ICE HRM [01;31m[K23[m[K.0 - Multiple Vulnerabilities
| php/webapps/46548.txt

Icecast 2.x - XSL Parser Multiple Vulnerabilities
| multiple/remote/25[01;31m[K23[m[K8.txt

iconics genesis32 and genesis64 - Multiple Vulnerabilities
| windows/dos/170[01;31m[K23[m[K.txt

ICQ 2003 - Webfront Guestbook Cross-Site Scripting
| asp/webapps/[01;31m[K23[m[K120.txt

IDA Pro 6.3 - Crash (PoC)
| multiple/dos/[01;31m[K23[m[K524.c

IdealBB 1.4.9 Beta - HTML Injection
| asp/webapps/[01;31m[K23[m[K055.txt

IDevSpot BizDirectory 2.04 - 'page' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K12.txt

IDevSpot PHPLinkExchange 1.01/1.02 - 'index.php' Multiple Cross-Site
Scripting Vulnerabilities             |
php/webapps/32[01;31m[K23[m[K0.txt

IGeneric Free Shopping Cart 1.4 - Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K773.txt

IGeneric Free Shopping Cart 1.4 - SQL Injection
| php/webapps/[01;31m[K23[m[K770.txt

Ilia Alshanetsky FUDForum 1.2.8/1.9.8/2.0.2 - File Disclosure
| php/webapps/217[01;31m[K23[m[K.txt

ImpressCMS 1.3.11 - 'bid' SQL Injection
| php/webapps/46[01;31m[K23[m[K9.txt

In-link 2.3.4/5.1.3 RC1 - 'cat' SQL Injection
| php/webapps/361[01;31m[K23[m[K.txt

In-portal 5.0.3 - Arbitrary File Upload
| php/webapps/1[01;31m[K23[m[K50.txt

INCOGEN Bugport 1.x - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                           |
php/webapps/270[01;31m[K23[m[K.txt
```

```
InduSoft Web Studio - 'ISSymbol.ocx InternationalSeparator()' Heap
Overflow (Metasploit)                    |
windows/remote/[01;31m[K23[m[K500.rb

Inetserv 3.[01;31m[K23[m[K - SMTP Denial of Service
| windows/dos/16035.py

Inetserv 3.[01;31m[K23[m[K POP3 - Denial of Service
| windows/dos/16038.py

Inmatrix Ltd. Zoom Player 8.5 - '.jpeg'File Memory Corruption /
Arbitrary Code Execution                   |
windows/local/[01;31m[K23[m[K996.py

Inside Systems Mail 2.0 - 'error.php' Cross-Site Scripting
| php/webapps/292[01;31m[K23[m[K.txt

IntelliTamper 2.07/2.08 Beta 4 - A HREF Remote Buffer Overflow
| windows/remote/6[01;31m[K23[m[K8.c

InterAKT Online MX Shop 1.1.1 - SQL Injection
| php/webapps/253[01;31m[K23[m[K.txt

Interchange 4.8.x/5.0 - Remote Information Disclosure
| asp/webapps/[01;31m[K23[m[K895.txt

International TeleCommunications WebBBS 2.13 - login & Password Buffer
Overflow                             |
windows/remote/196[01;31m[K23[m[K.c

Internet Security Systems ICECap Manager 2.0.[01;31m[K23[m[K - Default
Username and Password                          |
windows/remote/19922.pl

Internet Security Systems Protocol Analysis Module ICQ - Parsing Buffer
Overflow                           |
windows/remote/[01;31m[K23[m[K847.c

InternetNow ProxyNow 2.6/2.75 - Multiple Stack / Heap Overflow
Vulnerabilities                              |
windows/remote/[01;31m[K23[m[K608.pl

Internship Portal Management System 1.0 - Remote Code
Execution(Unauthenticated)                             |
php/webapps/498[01;31m[K23[m[K.py

Invision Power Board (IP.Board) 1.0/1.1/1.2 - 'admin.php' Cross-Site
Scripting                              |
php/webapps/[01;31m[K23[m[K001.txt

Invision Power Board (IP.Board) 1.3 - 'Pop' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K795.txt
```

Invision Power Board (IP.Board) 1.3 - Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/[01;31m[K23[m[K767.txt

Invision Power Board (IP.Board) 1.x - 'index.php' showtopic Cross-Site Scripting |
php/webapps/[01;31m[K23[m[K129.txt

Invision Power Board (IP.Board) 3.3.4 - 'Unserialize()' PHP Code Execution |
php/webapps/2[01;31m[K23[m[K98.php

Invision Power Board - Denial of Service
| multiple/dos/1[01;31m[K23[m[K82.txt

Invision Power Services Invision Gallery 1.0.1 - Multiple SQL Injections |
php/webapps/[01;31m[K23[m[K867.txt

Invision Power Top Site List 1.0/1.1 - 'id' SQL Injection
| php/webapps/[01;31m[K23[m[K868.txt

iOS 7 - Kernel Mode Memory Corruption
| ios/dos/3[01;31m[K23[m[K33.txt

iOS Share 1.0 - Directory Traversal
| ios/remote/16[01;31m[K23[m[K1.txt

IP3 Networks IP3 NetAccess Appliance - SQL Injection
| hardware/remote/[01;31m[K23[m[K808.txt

IPFire < 2.19 Update Core 110 - Remote Code Execution (Metasploit)
| cgi/remote/4[01;31m[K23[m[K69.rb

iPhone Guitar - Directory Traversal
| hardware/remote/16[01;31m[K23[m[K9.txt

iphone ishred 1.93 - Directory Traversal
| hardware/remote/16[01;31m[K23[m[K8.txt

IPSwitch IMail Server 2006 - SEARCH Remote Stack Overflow
| windows/remote/42[01;31m[K23[m[K.pl

Ipswitch Imail Server 5.0 - SMTP HELO Argument Buffer Overflow
| windows/dos/[01;31m[K23[m[K145.c

Ipswitch WS_FTP Server 3.4/4.0 - FTP Command Buffer Overrun
| windows/remote/[01;31m[K23[m[K100.c

IPUX CS7522/CS[01;31m[K23[m[K30/CS2030 IP Camera - 'UltraHVCamX.ocx' ActiveX Stack Buffer Overflow |
hardware/remote/35422.txt

IRCnet IRCD 2.10 - Local Buffer Overflow
| linux/dos/[01;31m[K23[m[K[01;31m[K23[m[K9.c

IrfanView 4.33 - 'IMXCF.dll' Plugin Code Execution
| windows/dos/[01;31m[K23[m[K288.txt

irokez blog 0.7.3.2 - Cross-Site Scripting / Remote File Inclusion / Blind SQL Injection |
php/webapps/81[01;31m[K23[m[K.txt

Irokez Blog 0.7.3.2 - Multiple Input Validation Vulnerabilities
| php/webapps/328[01;31m[K23[m[K.txt

ISC BIND 9 - TKEY Remote Denial of Service (PoC)
| multiple/dos/377[01;31m[K23[m[K.py

iSoft-Solutions QuikStore Shopping Cart 2.12 - 'store' Full Path Disclosure |
cgi/webapps/[01;31m[K23[m[K466.txt

iSoft-Solutions QuikStore Shopping Cart 2.12 - 'template' Directory Traversal |
cgi/webapps/[01;31m[K23[m[K467.txt

ISPworker 1.[01;31m[K23[m[K - Remote File Disclosure
| linux/webapps/10262.txt

Itech Movie Portal Script 7.37 - SQL Injection
| php/webapps/41[01;31m[K23[m[K0.txt

Itech Multi Vendor Script 6.49 - SQL Injection
| php/webapps/41[01;31m[K23[m[K8.txt

Itech Travel Portal Script 9.33 - SQL Injection
| php/webapps/410[01;31m[K23[m[K.txt

Itech Travel Portal Script 9.35 - SQL Injection
| php/webapps/41[01;31m[K23[m[K1.txt

iyzi Forum 1.0 Beta 3 - SQL Injection
| asp/webapps/24[01;31m[K23[m[K.txt

J. River Media Center 11.0.309 - Remote Denial of Service (PoC)
| windows/dos/[01;31m[K23[m[K02.pl

Jamit Job Board 3.x - Blind SQL Injection
| php/webapps/7[01;31m[K23[m[K5.txt

Jamroom 4.0.2 - 't' Local File Inclusion
| php/webapps/84[01;31m[K23[m[K.txt

Jason Maloney's Guestbook 3.0 - Remote Command Execution
| cgi/webapps/[01;31m[K23[m[K409.c

```
JasperReports - (Authenticated) File Read
| multiple/webapps/446[01;31m[K23[m[K.txt

Java - Web Start Double Quote Injection Remote Code Execution
(Metasploit)                                    |
multiple/remote/261[01;31m[K23[m[K.rb

Java-springboot-codebase 1.1 - Arbitrary File Read
| java/webapps/5[01;31m[K23[m[K04.py

Jaw Portal 1.2 - 'index.php' Multiple Local File Inclusions
| php/webapps/3[01;31m[K23[m[K51.txt

JBoss 3.0.8/3.2.1 - HSQLDB Remote Command Injection
| multiple/remote/[01;31m[K23[m[K221.txt

JBrowser 1.0/2.x - 'browser.php' Directory Traversal
| php/webapps/[01;31m[K23[m[K618.txt

JBrowser 1.0/2.x - Unauthorized Admin Access
| php/webapps/[01;31m[K23[m[K628.txt

Jedox 2022.4.2 - Code Execution via RPC Interfaces
| php/webapps/514[01;31m[K23[m[K.txt

Jenkins 1.5[01;31m[K23[m[K - Persistent HTML Code
| php/webapps/30408.txt

Jenkins 2.[01;31m[K23[m[K5.3 - 'Description' Stored XSS
| java/webapps/49[01;31m[K23[m[K7.txt

Jenkins 2.[01;31m[K23[m[K5.3 - 'tooltip' Stored Cross-Site Scripting
| java/webapps/49[01;31m[K23[m[K2.txt

Jenkins 2.[01;31m[K23[m[K5.3 - 'X-Forwarded-For' Stored XSS
| java/webapps/49244.txt

Jenkins < 1.650 - Java Deserialization
| java/remote/4[01;31m[K23[m[K94.py

JetBrains TeamCity 20[01;31m[K23[m[K.05.3 - Remote Code Execution (RCE)
| java/remote/51884.py

Jinzora 2.7.5 - 'ajax_request.php' Multiple Cross-Site Scripting
Vulnerabilities                              |
php/webapps/31[01;31m[K23[m[K6.txt

Jinzora 2.7.5 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                                   |
php/webapps/31[01;31m[K23[m[K5.txt
```

Jinzora 2.7.5 - 'popup.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/31[01;31m[K23[m[K8.txt

Jinzora 2.7.5 - 'slim.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/31[01;31m[K23[m[K7.txt

John Beatty Easy PHP Photo Album 1.0 - 'dir' HTML Injection | php/webapps/[01;31m[K23[m[K338.txt

Joomla! 1.5.x - 'Token' Remote Admin Change Password | php/webapps/6[01;31m[K23[m[K4.txt

Joomla! Component ACYMAILING 3.9.0 - Unauthenticated Arbitrary File Upload | php/webapps/48[01;31m[K23[m[K0.txt

Joomla! Component AJAX Shoutbox 1.6 - SQL Injection | php/webapps/3[01;31m[K23[m[K31.txt

Joomla! Component Answers 2.3beta - Multiple Vulnerabilities | php/webapps/139[01;31m[K23[m[K.txt

Joomla! Component BeeHeard 1.0 - Local File Inclusion | php/webapps/12[01;31m[K23[m[K9.txt

Joomla! Component CCNewsLetter 2.1.9 - 'sbid' SQL Injection | php/webapps/4[01;31m[K23[m[K87.txt

Joomla! Component com_avosbillets - SQL Injection | php/webapps/112[01;31m[K23[m[K.txt

Joomla! Component com_casino - SQL Injection | php/webapps/11[01;31m[K23[m[K7.txt

Joomla! Component com_ContentBlogList - SQL Injection | php/webapps/11[01;31m[K23[m[K6.txt

Joomla! Component com_gcalendar 1.1.2 - 'gcid' SQL Injection | php/webapps/10[01;31m[K23[m[K2.txt

Joomla! Component com_jbpublishdownfp - SQL Injection | php/webapps/11[01;31m[K23[m[K8.txt

Joomla! Component com_jbudgetsmagic 0.3.2 < 0.4.0 - 'bid' SQL Injection | multiple/webapps/97[01;31m[K23[m[K.txt

Joomla! Component com_Joomlaoads - 'packageId' SQL Injection | php/webapps/9[01;31m[K23[m[K8.txt

Joomla! Component com_jooproperty 1.13.0 - Multiple Vulnerabilities | php/webapps/[01;31m[K23[m[K286.txt

Joomla! Component com_lyftenbloggie 1.04 - SQL Injection
| php/webapps/10[01;31m[K23[m[K8.txt

Joomla! Component com_pcchess - Local File Inclusion
| php/webapps/121[01;31m[K23[m[K.txt

Joomla! Component com_portfolio - Local File Disclosure
| php/webapps/1[01;31m[K23[m[K25.txt

Joomla! Component com_s5clanroster - Local File Inclusion
| php/webapps/12[01;31m[K23[m[K1.txt

Joomla! Component com_spa - SQL Injection (1)
| php/webapps/144[01;31m[K23[m[K.txt

Joomla! Component com_wgpicasa - Local File Inclusion
| php/webapps/12[01;31m[K23[m[K0.txt

Joomla! Component Delicious Bookmarks 0.0.1 - Local File Inclusion
| php/webapps/12[01;31m[K23[m[K7.txt

Joomla! Component Deluxe Blog Factory 1.1.2 - Local File Inclusion
| php/webapps/12[01;31m[K23[m[K8.txt

Joomla! Component equotes 0.9.4 - SQL Injection
| php/webapps/57[01;31m[K23[m[K.txt

Joomla! Component Event Booking 2.10.1 - SQL Injection
| php/webapps/404[01;31m[K23[m[K.txt

Joomla! Component Ignite Gallery 0.8.3 - SQL Injection
| php/webapps/67[01;31m[K23[m[K.txt

Joomla! Component J-BusinessDirectory 4.9.7 - 'type' SQL Injection
| php/webapps/46[01;31m[K23[m[K0.txt

Joomla! Component J-ClassifiedsManager 3.0.5 - SQL Injection
| php/webapps/46[01;31m[K23[m[K1.txt

Joomla! Component J-CruisePortal 6.0.4 - SQL Injection
| php/webapps/46[01;31m[K23[m[K3.txt

Joomla! Component JA Comment - Local File Inclusion
| php/webapps/12[01;31m[K23[m[K6.txt

Joomla! Component JBDiary - Blind SQL Injection
| php/webapps/11[01;31m[K23[m[K9.txt

Joomla! Component JBuildozer 1.4.1 - 'appid' SQL Injection
| php/webapps/433[01;31m[K23[m[K.txt

Joomla! Component JCK Editor 6.4.4 - 'parent' SQL Injection
| php/webapps/454[01;31m[K23[m[K.txt

Joomla! Component JHotelReservation 6.0.7 - SQL Injection
| php/webapps/46[01;31m[K23[m[K4.txt

Joomla! Component JInventory 1.[01;31m[K23[m[K.02 - Local File
Inclusion |
php/webapps/12065.txt

Joomla! Component JMultipleHotelReservation 6.0.7 - SQL Injection
| php/webapps/46[01;31m[K23[m[K2.txt

Joomla! Component JoomlaFacebook - SQL Injection
| php/webapps/33[01;31m[K23[m[K8.txt

Joomla! Component JoomRecipe 1.0.4 - 'search_author' SQL Injection
| php/webapps/4[01;31m[K23[m[K47.txt

Joomla! Component JPodium 2.7.3 - SQL Injection
| php/webapps/14[01;31m[K23[m[K2.txt

Joomla! Component JS Jobs (com_jsjobs) 1.2.5 - 'cities.php' SQL
Injection |
php/webapps/47[01;31m[K23[m[K2.txt

Joomla! Component JS Support Ticket (com_jssupportticket) 1.1.6 -
'ticket.php' Arbitrary File Deletion |
php/webapps/472[01;31m[K23[m[K.txt

Joomla! Component JTM Reseller 1.9 Beta - SQL Injection
| php/webapps/1[01;31m[K23[m[K06.txt

Joomla! Component Love Factory 1.3.4 - Local File Inclusion
| php/webapps/12[01;31m[K23[m[K5.txt

Joomla! Component Media Mall Factory 1.0.4 - Blind SQL Injection
| php/webapps/12[01;31m[K23[m[K4.txt

Joomla! Component MMS Blog 2.3.0 - Local File Inclusion
| php/webapps/1[01;31m[K23[m[K18.txt

Joomla! Component MT Fire Eagle 1.2 - Local File Inclusion
| php/webapps/12[01;31m[K23[m[K3.txt

Joomla! Component NeoRecruit 4.1 - SQL Injection
| php/webapps/441[01;31m[K23[m[K.txt

Joomla! Component onisQuotes 2.5 - 'tag' SQL Injection
| php/webapps/413[01;31m[K23[m[K.txt

Joomla! Component Online News Paper Manager 1.0 - 'cid' SQL Injection
| php/webapps/1[01;31m[K23[m[K05.txt

Joomla! Component OrgChart 1.0.0 - Local File Inclusion
| php/webapps/1[01;31m[K23[m[K17.txt

Joomla! Component Photo Battle 1.0.1 - Local File Inclusion
| php/webapps/12[01;31m[K23[m[K2.txt

Joomla! Component ProductShowcase 1.5 - SQL Injection
| php/webapps/5[01;31m[K23[m[K7.txt

Joomla! Component Q-Personel 1.0 - SQL Injection
| php/webapps/127[01;31m[K23[m[K.py

Joomla! Component redSHOP 1.0.[01;31m[K23[m[K.1 - Blind SQL Injection
| php/webapps/14368.txt

Joomla! Component simpledownload 0.9.5 - Local File Disclosure
| php/webapps/126[01;31m[K23[m[K.txt

Joomla! Component Spider Calendar - 'date' Blind SQL Injection
| php/webapps/[01;31m[K23[m[K782.txt

Joomla! Component SportFusion 0.2.x - SQL Injection
| php/webapps/33[01;31m[K23[m[K7.txt

Joomla! Component StreetGuessr Game 1.1.8 - SQL Injection
| php/webapps/424[01;31m[K23[m[K.txt

Joomla! Component vBizz 1.0.7 - SQL Injection
| php/webapps/462[01;31m[K23[m[K.txt

Joomla! Component WMI 1.5.0 - Local File Inclusion
| php/webapps/1[01;31m[K23[m[K16.txt

Jorani v1.0.3-(c)2014-20[01;31m[K23[m[K - XSS Reflected & Information
Disclosure |
php/webapps/51715.txt

Jordan Windows Telnet Server 1.0/1.2 - 'Username' Stack Buffer Overrun
(1) |
windows/remote/[01;31m[K23[m[K491.pl

Jordan Windows Telnet Server 1.0/1.2 - 'Username' Stack Buffer Overrun
(2) |
windows/remote/[01;31m[K23[m[K492.c

Jordan Windows Telnet Server 1.0/1.2 - 'Username' Stack Buffer Overrun
(3) |
windows/remote/[01;31m[K23[m[K493.txt

Juju-run Agent - Privilege Escalation (Metasploit)
| linux/local/440[01;31m[K23[m[K.rb

Justin Hagstrom Auto Directory Index 1.2.3 - Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K386.txt

KAME Racoon - 'Initial Contact' SA Deletion
| freebsd/dos/[01;31m[K23[m[K540.c

Kardex Mlog MCC 5.7.12 - RCE (Remote Code Execution)
| windows/remote/51[01;31m[K23[m[K9.py

KarjaSoft Sami HTTP Server 1.0.4 - GET Buffer Overflow
| windows/remote/[01;31m[K23[m[K714.c

Kasseler CMS 2 r12[01;31m[K23[m[K - Multiple Vulnerabilities
| php/webapps/266[01;31m[K23[m[K.txt

KDPics 1.18 - '/admin/index.php' Authentication Bypass
| php/webapps/337[01;31m[K23[m[K.html

Kebi Academy 2001 - Input Validation
| cgi/webapps/2[01;31m[K23[m[K77.txt

Keeper Security desktop 16.10.2 & Browser Extension 16.5.4 - Password Dumping |
multiple/local/516[01;31m[K23[m[K.cs

Kentico CMS 5.5R2.[01;31m[K23[m[K - 'userContextMenu_Parameter' Cross-Site Scripting |
asp/webapps/35807.txt

Kerio Personal Firewall 4.0.x - Web Filtering Remote Denial of Service
| windows/dos/[01;31m[K23[m[K925.txt

Key Focus Web Server 3.1 - Index.WKF Cross-Site Scripting
| multiple/remote/30[01;31m[K23[m[K1.txt

Kietu 2/3 - 'index.php' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K607.txt

KikChat - Local File Inclusion / Remote Code Execution
| php/webapps/30[01;31m[K23[m[K5.txt

KingMedia 4.1 - File Upload
| php/webapps/45[01;31m[K23[m[K7.php

Kingsoft Webshield 'KAVSafe.sys' 2010.4.14.609 (2010.5.[01;31m[K23[m[K) - Kernel Mode Privilege Escalation | windows/local/12710.c

KnowledgeBuilder 2.0/2.1/3.0 - Remote File Inclusion
| php/webapps/[01;31m[K23[m[K476.txt

KnowledgeBuilder 2.2 - 'visEdit_root' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K64.txt

Koch Roland Rolis Guestbook 1.0 - '$path' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K384.txt

```
Kordil EDms 2.2.60rc3 - SQL Injection
| php/webapps/[01;31m[K23[m[K180.txt

Kostenloses Linkmanagementscript - SQL Injection
| php/webapps/56[01;31m[K23[m[K.txt

kpopup 0.9.x - Privileged Command Execution
| linux/local/[01;31m[K23[m[K308.c

Kroum Grigorov KpyM Telnet Server 1.0 - Remote Denial of Service
| windows/dos/[01;31m[K23[m[K530.c

Ksemail - Local File Inclusion
| php/webapps/54[01;31m[K23[m[K.txt

KsIRC 1.3.12 - 'PRIVMSG' Remote Buffer Overflow (PoC)
| linux/dos/30[01;31m[K23[m[K.c

Kukol E.V. HTTP & FTP Server Suite 6.2 - File Disclosure
| windows/remote/[01;31m[K23[m[K121.txt

KwsPHP 1.0 Module Newsletter - SQL Injection
| php/webapps/45[01;31m[K23[m[K.pl

Kyocera Mita Scanner File Utility 3.3.0.1 - File Transfer Directory
Traversal                                 |
windows/remote/3[01;31m[K23[m[K01.py

L-Soft 1.8 - Listserv Multiple Cross-Site Scripting Vulnerabilities
| cgi/webapps/[01;31m[K23[m[K485.txt

LabCollector 5.4[01;31m[K23[m[K - SQL Injection
| php/webapps/47460.txt

LabF nfsAxe FTP Client 3.7 - Remote Buffer Overflow (DEP Bypass)
| windows/remote/43[01;31m[K23[m[K6.py

LAME 3.99.5 - Multiple Vulnerabilities
| linux/dos/4[01;31m[K23[m[K90.txt

Land Down Under 601/602/700/701/800/801 - 'events.php' HTML Injection
| php/webapps/262[01;31m[K23[m[K.txt

LANDesk Lenovo ThinkManagement Suite 9.0.3 Core Server - Arbitrary File
Deletion                              |
windows/remote/186[01;31m[K23[m[K.txt

lanewsfactory - Multiple Vulnerabilities
| php/webapps/1[01;31m[K23[m[K61.txt

LAquis SCADA 4.1.0.[01;31m[K23[m[K85 - Directory Traversal (Metasploit)
| multiple/remote/42885.rb
```

```
Laravel Pulse 1.3.1 - Arbitrary Code Injection
| php/webapps/5[01;31m[K23[m[K19.py

lastore-daemon D-Bus - Privilege Escalation (Metasploit)
| linux/local/445[01;31m[K23[m[K.rb

Laurent Adda Les Commentaires 2.0 - PHP Script 'admin.php' Remote File
Inclusion                          |
php/webapps/[01;31m[K23[m[K621.txt

Laurent Adda Les Commentaires 2.0 - PHP Script
'derniers_commentaires.php' Remote File Inclusion          |
php/webapps/[01;31m[K23[m[K620.txt

Laurent Adda Les Commentaires 2.0 - PHP Script 'fonctions.lib.php'
Remote File Inclusion                  |
php/webapps/[01;31m[K23[m[K619.txt

LBlog 1.05 - 'comments.asp' SQL Injection
| asp/webapps/2[01;31m[K23[m[K0.txt

lcdproc lcdd 0.x/4.x - Multiple Vulnerabilities
| linux/remote/[01;31m[K23[m[K936.pl

Ledscripts LedForums - Multiple HTML Injections
| php/webapps/[01;31m[K23[m[K313.txt

Leif M. Wright Web Blog 1.1 - File Disclosure
| cgi/webapps/[01;31m[K23[m[K613.txt

Leif M. Wright Web Blog 1.1 - Remote Command Execution
| cgi/webapps/[01;31m[K23[m[K629.txt

Les Visiteurs 2.0 - Remote File Inclusion
| php/webapps/[01;31m[K23[m[K302.txt

LGames LBreakout2 2.2.2 - Multiple Environment Variable Buffer Overflow
Vulnerabilities                    | linux/local/[01;31m[K23[m[K738.c

libdbus - 'DBUS_SYSTEM_BUS_ADDRESS' Local Privilege Escalation
| linux/local/213[01;31m[K23[m[K.c

libjpeg-turbo 1.5.1 - Denial of Service
| linux/dos/4[01;31m[K23[m[K91.txt

Library Management System 2.0 - Auth Bypass SQL Injection
| php/webapps/49[01;31m[K23[m[K0.txt

LibTIFF - 'tif_jbig.c' Denial of Service
| linux/dos/4[01;31m[K23[m[K00.txt

LibTIFF - '_TIFFVGetField (tiffsplit)' Out-of-Bounds Read
| linux/dos/4[01;31m[K23[m[K01.txt
```

```
libvorbis 1.3.5 - Multiple Vulnerabilities
| linux/dos/4[01;31m[K23[m[K99.txt

libxslt XSL 1.1.[01;31m[K23[m[K - File Processing Buffer Overflow
| linux/dos/31815.html

LightDM (Ubuntu 16.04/16.10) - 'Guest Account' Local Privilege
Escalation                                |
linux/local/419[01;31m[K23[m[K.txt

LightNEasy 3.1.x - Multiple Vulnerabilities
| php/webapps/1[01;31m[K23[m[K22.txt

LightNEasy sql/no-db 2.2.x - System Configuration Disclosure
| php/webapps/89[01;31m[K23[m[K.py

Lighttpd < 1.4.[01;31m[K23[m[K (BSD/Solaris) - Source Code Disclosure
| multiple/remote/8786.txt

Limbo CMS 1.0.4.2L - 'com_contact' Remote Code Execution
| php/webapps/[01;31m[K23[m[K70.php

LimeSurvey 4.1.11 - 'Permission Roles' Persistent Cross-Site Scripting
| php/webapps/485[01;31m[K23[m[K.txt

LinBit Technologies LINBOX Officeserver - Remote Authentication Bypass
| cgi/webapps/[01;31m[K23[m[K897.txt

Link CMS - 'navigacija.php?IDMeniGlavni' SQL Injection
| php/webapps/29[01;31m[K23[m[K2.txt

Link CMS - 'prikazInformacije.php?IDStranicaPodaci' SQL Injection
| php/webapps/29[01;31m[K23[m[K3.txt

linksnet newsfeed 1.0 - Remote File Inclusion
| php/webapps/39[01;31m[K23[m[K.txt

Linksys WAP55AG 1.0.7 - SNMP Community String Insecure Configuration
| hardware/remote/[01;31m[K23[m[K721.txt

Linux - Use-After-Free Reads in show_numa_stats()
| linux/dos/47[01;31m[K23[m[K6.c

Linux Kernel (Debian 7/8/9/10 / Fedora [01;31m[K23[m[K/24/25 / CentOS
5.3/5.11/6.0/6.8/7.2.1511) - 'ldso_hwcap Stack Cl |
linux_x86/local/42274.c

Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora
[01;31m[K23[m[K/24/25) - 'ldso_dynamic Stack Clash' L |
linux_x86/local/42276.c

Linux Kernel 2.2 - TCP/IP Spoof IP
| linux/remote/[01;31m[K23[m[K7.c
```

Linux Kernel 2.2.x/2.4.x - Privileged Process Hijacking Privilege Escalation (1) | linux/local/2[01;31m[K23[m[K62.c

Linux Kernel 2.2.x/2.4.x - Privileged Process Hijacking Privilege Escalation (2) | linux/local/2[01;31m[K23[m[K63.c

Linux Kernel 2.4.[01;31m[K23[m[K/2.6.0 - 'do_mremap()' Bound Checking Privilege Escalation | linux/local/145.c

Linux Kernel 2.4.[01;31m[K23[m[K/2.6.0 - 'do_mremap()' Bound Checking Validator (1) | linux/local/141.c

Linux Kernel 2.4.[01;31m[K23[m[K/2.6.0 - 'do_mremap()' Bound Checking Validator (2) | linux/local/142.c

Linux Kernel 2.4.x/2.6.x - Multiple ISO9660 Filesystem Handling Vulnerabilities | linux/dos/25[01;31m[K23[m[K4.sh

Linux Kernel 2.4/2.6 - Sigqueue Blocking Denial of Service | linux/dos/[01;31m[K23[m[K946.c

Linux Kernel 2.6.[01;31m[K23[m[K < 2.6.24 - 'vmsplice' Local Privilege Escalation (1) | linux/local/5093.c

Linux Kernel 2.6.24_16-[01;31m[K23[m[K/2.6.27_7-10/2.6.28.3 (Ubuntu 8.04/8.10 / Fedora Core 10 x86-64) - 'set_selection | linux_x86-64/local/9083.c

Linux Kernel 2.6.x - 'add_to_page_cache_lru()' Local Denial of Service | linux/dos/3[01;31m[K23[m[K84.txt

Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'mct_u[01;31m[K23[m[K2' Nullpointer Dereference | linux/dos/39541.txt

Linux Kernel 3.2.0-[01;31m[K23[m[K/3.5.0-[01;31m[K23[m[K (Ubuntu 12.04/12.04.1/12.04.2 x64) - 'perf_swevent_init' Local Privilege Es | linux_x86-64/local/33589.c

Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free | linux/dos/43[01;31m[K23[m[K4.c

Linux Kernel 4.3.3 - 'overlayfs' Local Privilege Escalation (2) | linux/local/39[01;31m[K23[m[K0.c

Linux Kernel 4.8.0 UDEV < [01;31m[K23[m[K2 - Local Privilege Escalation | linux/local/41886.c

Linux Kernel < 2.6.28 - 'fasync_helper()' Local Privilege Escalation | linux/local/335[01;31m[K23[m[K.c

Linux Kernel < 2.6.36-rc4-git2 (x86-64) - 'ia32syscall' Emulation Privilege Escalation | linux_x86-64/local/150[01;31m[K23[m[K.c

Linux Kernel < 3.16.1 - 'Remount FUSE' Local Privilege Escalation | linux/local/349[01;31m[K23[m[K.c

Linux Kernel < 3.2.0-[01;31m[K23[m[K (Ubuntu 12.04 x64) - 'ptrace/sysret' Local Privilege Escalation | linux_x86-64/local/34134.c

Linux Kernel < 3.5.0-[01;31m[K23[m[K (Ubuntu 12.04.2 x64) - 'SOCK_DIAG' SMEP Bypass Local Privilege Escalation | linux_x86-64/local/44299.c

Linux VServer Project 1.2x - Chroot Breakout | linux/local/[01;31m[K23[m[K658.c

LionMax Software WWW File Share Pro 2.4/2.6 - Remote Denial of Service | windows/dos/[01;31m[K23[m[K538.txt

lionmax software www file share pro 2.4x - Multiple Vulnerabilities (1) | multiple/remote/[01;31m[K23[m[K541.c

lionmax software www file share pro 2.4x - Multiple Vulnerabilities (2) | multiple/remote/[01;31m[K23[m[K542.c

Liquid War 5.4.5/5.5.6 - HOME Environment Variable Buffer Overflow | linux/remote/[01;31m[K23[m[K151.c

Lisk CMS 4.4 - 'id' Multiple Cross-Site Scripting / SQL Injections | php/webapps/340[01;31m[K23[m[K.txt

ListMessenger 0.9.3 - 'LM_Path' Remote File Inclusion | php/webapps/28[01;31m[K23[m[K1.txt

Litespeed Cache WordPress Plugin 6.3.0.1 - Privilege Escalation | php/webapps/5[01;31m[K23[m[K28.py

Litespeed Web Server 4.0.17 with PHP (FreeBSD) - Remote Overflow | freebsd/remote/157[01;31m[K23[m[K.pl

LiteSpeed Web Server Enterprise 5.4.11 - Command Injection (Authenticated) | php/webapps/495[01;31m[K23[m[K.txt

LiteWEB Web Server 2.7 - Invalid Page Remote Denial of Service | windows/dos/30[01;31m[K23[m[K3.pl

LiveJournal 1.1 - CSS HTML Injection | php/webapps/[01;31m[K23[m[K749.txt

LiveZilla 3.1.8.3 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/34[01;31m[K23[m[K1.txt

Loadbalancer.org Enterprise VA 7.5.2 - Static SSH Key
| unix/remote/3[01;31m[K23[m[K71.txt

Logitech Media Server 7.9.0 - 'Radio URL' Cross-Site Scripting
| multiple/webapps/431[01;31m[K23[m[K.txt

Loom Software SurfNow 1.x/2.x - GET Remote Denial of Service
| windows/dos/[01;31m[K23[m[K614.txt

LoveCMS 1.6.2 Final (Download Manager 1.0) - Arbitrary File Upload
| php/webapps/7[01;31m[K23[m[K3.txt

LPRng 3.6.22/[01;31m[K23[m[K/24 - Remote Command Execution
| linux/remote/226.c

LPRng 3.6.24-1 - Remote Command Execution
| linux/remote/[01;31m[K23[m[K0.c

LPRng 3.6.x - Failure To Drop Supplementary Groups
| unix/local/209[01;31m[K23[m[K.c

LSH 1.x - Remote Buffer Overflow (1)
| linux/remote/[01;31m[K23[m[K161.c

LSH 1.x - Remote Buffer Overflow (2)
| linux/remote/[01;31m[K23[m[K162.c

m0n0wall 1.33 - Multiple Cross-Site Request Forgery Vulnerabilities
| freebsd/webapps/[01;31m[K23[m[K202.txt

M3U/M3L to ASX/WPL 1.1 - '.asx' / '.m3u' / '.m3l' Local Buffer Overflow
(PoC) | windows/dos/91[01;31m[K23[m[K.pl

Mabry Software FTPServer/X 1.0 - Controls Format String
| linux/dos/[01;31m[K23[m[K539.txt

Macallan Mail Solution Macallan Mail Solution 2.8.4.6 (Build 260) - Web
Interface Authentication Bypass | php/webapps/[01;31m[K23[m[K687.txt

macOS - 'sysctl_vfs_generic_conf' Stack Leak Through Struct Padding
| macos/dos/439[01;31m[K23[m[K.c

macOS LaunchDaemon iOS 17.2 - Privilege Escalation
| macos/local/5[01;31m[K23[m[K16.py

Macromedia ColdFusion MX 6.0 - SQL Error Message Cross-Site Scripting
| cfm/webapps/[01;31m[K23[m[K256.txt

Macromedia Flash Player 6.0.x - Flash Cookie Predictable File Location
| windows/remote/[01;31m[K23[m[K298.txt

Macromedia JRun 4.0 build 61650 - Administrative Interface Multiple Cross-Site Scripting Vulnerabilities | jsp/webapps/[01;31m[K23[m[K402.txt

Madirish Webmail 2.01 - 'baseDir' Local/Remote File Inclusion | php/webapps/1[01;31m[K23[m[K69.txt

Mafya Oyun Scrpti - 'profil.php' SQL Injection | php/webapps/351[01;31m[K23[m[K.txt

Magic News Pro 1.0.3 - 'script_path' Remote File Inclusion | php/webapps/[01;31m[K23[m[K63.tt

Magic Photo Storage Website - '/user/couple_milestone.php?_config[site_path]' Remote File Inclusion | php/webapps/294[01;31m[K23[m[K.txt

magic-portal 2.1 - SQL Injection | php/webapps/11[01;31m[K23[m[K5.txt

MagicISO 5.4 (build[01;31m[K23[m[K9) - '.cue' File Local Buffer Overflow | windows/local/3975.c

MagicISO 5.4 (build[01;31m[K23[m[K9) - '.cue' Heap Overflow (PoC) | linux/dos/3945.rb

Mah-Jong 1.4 - Client/Server Remote sscanf() Buffer Overflow | linux/remote/[01;31m[K23[m[K115.c

Mah-Jong 1.4 - MJ-Player Server Flag Local Buffer Overflow | linux/local/[01;31m[K23[m[K197.c

Mah-Jong 1.4/1.6 - Server Remote Denial of Service | linux/dos/[01;31m[K23[m[K116.pl

MailEnable 1.501x - Email Server Buffer Overflow | windows/remote/220[01;31m[K23[m[K.c

MailEnable 3.13 SMTP Service - 'VRFY/EXPN' Denial of Service | windows/dos/5[01;31m[K23[m[K5.py

Mailman 1.x > 2.1.[01;31m[K23[m[K - Cross Site Scripting (XSS) | cgi/webapps/48970.txt

Mall[01;31m[K23[m[K - 'AddItem.asp' SQL Injection | asp/webapps/26291.txt

Mambo 4.5 Server - 'user.php' Script Unauthorized Access | php/webapps/[01;31m[K23[m[K428.html

Mambo Component com_loudmouth 4.0j - Remote File Inclusion | php/webapps/20[01;31m[K23[m[K.txt

```
Mambo Component com_registration_detailed 4.1 - Remote File Inclusion
| php/webapps/[01;31m[K23[m[K79.txt

Mambo Component com_serverstat 0.4.4 - Remote File Inclusion
| php/webapps/[01;31m[K23[m[K67.txt

Mambo Module Calendar 1.5.7 - 'Com_Calendar.php' Remote File Inclusion
| php/webapps/28[01;31m[K23[m[K3.txt

Mambo Open Source 4.0.14 - 'PollBooth.php' Multiple SQL Injections
| php/webapps/[01;31m[K23[m[K430.txt

Mambo Open Source 4.0.14 Server - SQL Injection
| php/webapps/[01;31m[K23[m[K429.txt

Mambo Open Source 4.5 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                          |
php/webapps/[01;31m[K23[m[K824.txt

Mambo Open Source 4.5 - 'index.php' SQL Injection
| php/webapps/[01;31m[K23[m[K834.txt

Mambo Open Source 4.5 - 'index.php?mos_change_template' Cross-Site
Scripting                                |
php/webapps/[01;31m[K23[m[K825.txt

Mambo Open Source 4.5/4.6 - 'mod_mainmenu.php' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K553.php

Mambo Open Source 4.6 - 'Itemid' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K657.txt

Mambo Site Server 4.0.10 - 'index.php' Cross-Site Scripting
| php/webapps/2[01;31m[K23[m[K82.txt

Mambo Site Server 4.0.14 - 'banners.php?bid' SQL Injection
| php/webapps/[01;31m[K23[m[K158.txt

Mambo Site Server 4.0.14 - 'contact.php' Unauthorized Mail Relay
| php/webapps/[01;31m[K23[m[K160.txt

Mambo Site Server 4.0.14 - 'emailarticle.php?id' SQL Injection
| php/webapps/[01;31m[K23[m[K159.txt

Man Program 1.5 - Unsafe Return Value Command Execution
| linux/local/2[01;31m[K23[m[K44.txt

Man Utility 2.3.19 - Local Compression Program Privilege Escalation
| linux/local/[01;31m[K23[m[K168.pl

Manage Engine Application Manager 12.5 - Arbitrary Command Execution
| multiple/webapps/39[01;31m[K23[m[K6.py
```

```
Manage Engine Applications Manager 12 - Multiple Vulnerabilities
| multiple/webapps/39[01;31m[K23[m[K5.txt

ManageEngine Desktop Central 10 Build 100087 - Remote Code Execution
(Metasploit)                              |
java/webapps/4[01;31m[K23[m[K58.rb

ManageEngine Security Manager Plus 5.5 build 5505 - SQL Injection
(Metasploit)                                |
multiple/remote/2[01;31m[K23[m[K04.rb

Mantis Bug Tracker 0.19.2/1.0 - 'Bug_sponsorship_list_view_inc.php'
File Inclusion                            |
php/webapps/264[01;31m[K23[m[K.txt

Mapbender 2.4.4 - 'gaz' SQL Injection
| php/webapps/5[01;31m[K23[m[K3.txt

Mapbender 2.4.4 - 'mapFiler.php' Remote Code Execution
| php/webapps/5[01;31m[K23[m[K2.txt

marbles 1.0.1 - Local Home Environment Variable Buffer Overflow
| linux/local/[01;31m[K23[m[K189.c

MathoPD 1.x - Remote Buffer Overflow
| linux/remote/[01;31m[K23[m[K811.c

MatrikzGB Guestbook 2.0 - Administrative Privilege Escalation
| php/webapps/[01;31m[K23[m[K036.txt

MAWK 1.3.3-17 - Local Buffer Overflow
| linux/local/4[01;31m[K23[m[K57.py

Maxthon3 - about:history XCS Trusted Zone Code Execution (Metasploit)
| windows/remote/[01;31m[K23[m[K225.rb

Maxtrade AIO 1.3.[01;31m[K23[m[K - 'categori' SQL Injection
| php/webapps/5853.txt

Maxwebportal 1.365 - 'forum.asp' SQL Injection
| asp/webapps/33[01;31m[K23[m[K6.txt

Maxwebportal 1.3x - 'down.asp' HTTP_REFERER Cross-Site Scripting
| asp/webapps/[01;31m[K23[m[K676.txt

Maxwebportal 1.3x - Personal Message 'SendTo' Cross-Site Scripting
| asp/webapps/[01;31m[K23[m[K677.txt

McAfee Asset Manager 6.6 - Multiple Vulnerabilities
| jsp/webapps/3[01;31m[K23[m[K68.txt
```

McAfee ePolicy Orchestrator 1.x/2.x/3.0 Agent - POST Buffer Mismanagement |
windows/dos/[01;31m[K23[m[K584.c

Mcafee FreeScan CoMcFreeScan Browser - Information Disclosure
| windows/remote/[01;31m[K23[m[K926.txt

Mcafee FreeScan CoMcFreeScan Browser - Object Buffer Overflow (PoC)
| windows/dos/[01;31m[K23[m[K920.txt

McGallery 1.0/1.1 - Lang Argument File Disclosure
| php/webapps/258[01;31m[K23[m[K.txt

mcGalleryPRO 2006 - 'path_to_folder' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K42.txt

McMurtrey/Whitaker & Associates Cart32 2-5 GetLatestBuilds Script - Cross-Site Scripting |
cgi/webapps/24[01;31m[K23[m[K6.txt

McNews 1.x - 'install.php' Arbitrary File Inclusion
| php/webapps/25[01;31m[K23[m[K2.txt

MD-Pro 1.0.76 - 'index.php' Firefox ID SQL Injection
| php/webapps/306[01;31m[K23[m[K.pl

MDaemon SMTP Server 5.0.5 - Null Password Authentication
| windows/remote/[01;31m[K23[m[K002.txt

MediaMonkey 4.1.[01;31m[K23[m[K - '.mp3' URL Denial of Service (PoC)
| windows/dos/46378.py

Medical Center Portal Management System 1.0 - Multiple Stored XSS
| php/webapps/49[01;31m[K23[m[K6.txt

Medieval Total War 1.0/1.1 - nickname Denial of Service
| multiple/dos/[01;31m[K23[m[K[01;31m[K23[m[K1.txt

Meet#Web 0.8 - 'ManagerResource.class.php?root_path' Remote File Inclusion |
php/webapps/32[01;31m[K23[m[K2.txt

Meet#Web 0.8 - 'ManagerRightsResource.class.php?root_path' Remote File Inclusion |
php/webapps/32[01;31m[K23[m[K3.txt

Meet#Web 0.8 - 'modules.php?root_path' Remote File Inclusion
| php/webapps/32[01;31m[K23[m[K1.txt

Meet#Web 0.8 - 'RegForm.class.php?root_path' Remote File Inclusion
| php/webapps/32[01;31m[K23[m[K4.txt

```
Meet#Web 0.8 - 'RegResource.class.php?root_path' Remote File Inclusion
| php/webapps/32[01;31m[K23[m[K5.txt

Meet#Web 0.8 - 'RegRightsResource.class.php?root_path' Remote File
Inclusion                                |
php/webapps/32[01;31m[K23[m[K6.txt

Mega File Hosting Script 1.2 - 'url' Remote File Inclusion
| php/webapps/8[01;31m[K23[m[K0.txt

MegaBrowser 0.3 - HTTP Directory Traversal
| windows/remote/227[01;31m[K23[m[K.txt

Megacubo 5.0.7 - 'mega://' Remote 'eval()' Injection
| windows/remote/76[01;31m[K23[m[K.html

MemHT Portal 4.0.1 - 'User Agent' Persistent Cross-Site Scripting
| php/webapps/156[01;31m[K23[m[K.pl

memorial Web site script - 'id' SQL Injection
| php/webapps/1[01;31m[K23[m[K51.txt

Memorial Web Site Script - Multiple Arbitrary Delete Vulnerabilities
| php/webapps/1[01;31m[K23[m[K59.txt

Memorial Web Site Script - Reset Password / Insecure Cookie Handling
| php/webapps/1[01;31m[K23[m[K58.txt

Mephistoles HTTPd 0.6 - Cross-Site Scripting
| multiple/remote/[01;31m[K23[m[K564.txt

Mercur MailServer 5.0 SP3 - 'IMAP' Remote Buffer Overflow (2)
| windows/remote/[01;31m[K23[m[K45.pl

Mercury/32 Mail Server 4.01a (Pegasus) - IMAP Buffer Overflow
| windows/remote/12[01;31m[K23[m[K.c

MetaDot Portal Server 5.6.x - 'index.pl' Multiple Cross-Site Scripting
Vulnerabilities                      |
cgi/webapps/[01;31m[K23[m[K550.txt

MetaDot Portal Server 5.6.x - 'index.pl' Multiple SQL Injections
| cgi/webapps/[01;31m[K23[m[K548.txt

MetaDot Portal Server 5.6.x - 'userchannel.pl?op' Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K551.txt

MetaDot Portal Server 5.6.x - index.pl Information Disclosure
| cgi/webapps/[01;31m[K23[m[K549.txt

Metamail 2.7 - Multiple Buffer Overflow / Format String Handling
Vulnerabilities                          |
linux/remote/[01;31m[K23[m[K728.txt
```

Metyus Forum Portal 1.0 - 'Philboard_Forum.asp' SQL Injection
| asp/webapps/304[01;31m[K23[m[K.txt

Michelles L2J Dropcalc 4 - SQL Injection
| php/webapps/3[01;31m[K23[m[K2.txt

Micropoint ProActive Denfense 'Mp110013.sys' 1.3.101[01;31m[K23[m[K.0 -
Local Privilege Escalation | windows/local/12213.c

Microsoft 365 MSO (Version [01;31m[K23[m[K05 Build 16.0.16501.20074)
32-bit - Remote Code Execution (RCE) |
multiple/remote/51555.txt

Microsoft 365 MSO (Version [01;31m[K23[m[K05 Build 16.0.16501.20074)
64-bit - Remote Code Execution (RCE) |
multiple/remote/51552.txt

Microsoft Access 97/2000/2002 Snapshot Viewer - ActiveX Control
Parameter Buffer Overflow |
windows/remote/[01;31m[K23[m[K095.c

Microsoft ActiveSync 3.5 - Null Pointer Dereference Denial of Service
| windows/dos/2[01;31m[K23[m[K90.c

Microsoft Edge 114.0.18[01;31m[K23[m[K.67 (64-bit) - Information
Disclosure |
multiple/local/51571.txt

Microsoft Edge 38.14393.0.0 - JavaScript Engine Use-After-Free
| windows/dos/416[01;31m[K23[m[K.html

Microsoft Edge Chakra JIT - Stack-to-Heap Copy
| windows/dos/437[01;31m[K23[m[K.js

Microsoft Excel 2010 - Crash (PoC) (1)
| windows/dos/2[01;31m[K23[m[K30.txt

Microsoft Excel 365 MSO (Version [01;31m[K23[m[K02 Build
16.0.16130.20186) 64-bit - Remote Code Execution (RCE) |
multiple/remote/51328.txt

Microsoft Excel Use After Free - Local Code Execution
| windows/local/5[01;31m[K23[m[K32.txt

Microsoft Exchange Server 4.0/5.0 - SMTP HELO Argument Buffer Overflow
| windows/remote/[01;31m[K23[m[K113.c

Microsoft IIS (Windows NT 4.0/SP1/SP2/SP3/SP4/SP5) - '.IDC' Path
Mapping |
windows/remote/19[01;31m[K23[m[K9.txt

Microsoft IIS 5.0 (Windows XP/2000/NT 4.0) - WebDAV 'ntdll.dll' Remote Buffer Overflow (1) | windows/remote/2[01;31m[K23[m[K65.pl

Microsoft IIS 5.0 (Windows XP/2000/NT 4.0) - WebDAV 'ntdll.dll' Remote Buffer Overflow (2) | windows/remote/2[01;31m[K23[m[K66.c

Microsoft IIS 5.0 (Windows XP/2000/NT 4.0) - WebDAV 'ntdll.dll' Remote Buffer Overflow (3) | windows/remote/2[01;31m[K23[m[K67.txt

Microsoft IIS 5.0 (Windows XP/2000/NT 4.0) - WebDAV 'ntdll.dll' Remote Buffer Overflow (4) | windows/remote/2[01;31m[K23[m[K68.txt

Microsoft IIS 5.0 - Failure To Log Undocumented TRACK Requests | windows/remote/[01;31m[K23[m[K490.txt

Microsoft IIS 5.0 - Printer Host Header Overflow (MS01-0[01;31m[K23[m[K) (Metasploit) | windows/remote/16469.rb

Microsoft IIS 5.1 - WebDAV HTTP Request Source Code Disclosure | windows/remote/26[01;31m[K23[m[K0.txt

Microsoft Internet Explorer - 'mshtml.dll' Remote Code Execution (MS17-007) | windows_x86-64/remote/4[01;31m[K23[m[K54.html

Microsoft Internet Explorer - 'Winhlp32.exe' MsgBox Code Execution (MS10-0[01;31m[K23[m[K) (Metasploit) | windows/remote/16541.rb

Microsoft Internet Explorer - CButton Object Use-After-Free (Metasploit) | windows/remote/[01;31m[K23[m[K785.rb

Microsoft Internet Explorer - CDwnBindInfo Object Use-After-Free (Metasploit) | windows/remote/[01;31m[K23[m[K754.rb

Microsoft Internet Explorer - COM Object Remote Heap Overflow | windows/remote/[01;31m[K23[m[K58.c

Microsoft Internet Explorer - MSHTML!CSVGHelpers::SetAttributeStringAndPointer Use-After-Free (MS16-0[01;31m[K23[m[K) | windows/dos/39663.html

Microsoft Internet Explorer - Multiple COM Object Color Property Denial of Service Vulnerabilities | windows/dos/2[01;31m[K23[m[K8.html

Microsoft Internet Explorer - Read AV in MSHTML!Layout::LayoutBuilderDivider::BuildPageLayout (MS16-0[01;31m[K23[m[K) | windows/dos/39562.html

Microsoft Internet Explorer 11 - Crash (PoC) (2) | windows/dos/37[01;31m[K23[m[K9.html

Microsoft Internet Explorer 11.0.9600.18617 - 'CMarkup::DestroySplayTree' Memory Corruption | windows/dos/4[01;31m[K23[m[K36.html

Microsoft Internet Explorer 11.1066.14393.0 - VBScript Arithmetic Functions Type Confusion | windows/dos/4[01;31m[K23[m[K37.html

Microsoft Internet Explorer 5 - Cascading Style Sheet File Disclosure (MS02-0[01;31m[K23[m[K) | windows/remote/21361.txt

Microsoft Internet Explorer 5 - NavigateAndFind() Cross-Zone Policy (MS04-004) | windows/remote/[01;31m[K23[m[K643.txt

Microsoft Internet Explorer 5 - Shell: IFrame Cross-Zone Scripting (1) | windows/remote/[01;31m[K23[m[K678.html

Microsoft Internet Explorer 5 - Shell: IFrame Cross-Zone Scripting (2) | windows/remote/[01;31m[K23[m[K679.html

Microsoft Internet Explorer 5 - window.open Search Pane Cross-Zone Scripting | windows/remote/[01;31m[K23[m[K790.html

Microsoft Internet Explorer 5 - XML Page Object Type Validation (MS03-040) | windows/remote/[01;31m[K23[m[K122.txt

Microsoft Internet Explorer 5.0.1 - ITS Protocol Zone Bypass (MS04-013) | windows/remote/[01;31m[K23[m[K695.txt

Microsoft Internet Explorer 5.0.1 - LoadPicture File Enumeration | windows/remote/[01;31m[K23[m[K668.txt

Microsoft Internet Explorer 5/6 - Browser Popup Window Object Type Validation | windows/remote/[01;31m[K23[m[K114.txt

Microsoft Internet Explorer 5/6 - Cross-Domain Event Leakage | windows/remote/[01;31m[K23[m[K766.html

Microsoft Internet Explorer 5/6 - Object Type Validation | windows/remote/[01;31m[K23[m[K044.txt

Microsoft Internet Explorer 5/6 / Mozilla 1.2.1 - URI Display Obfuscation (1) | windows/remote/[01;31m[K23[m[K422.txt

Microsoft Internet Explorer 5/6 / Mozilla 1.2.1 - URI Display Obfuscation (2) | windows/remote/[01;31m[K23[m[K4[01;31m[K23[m[K.txt

Microsoft Internet Explorer 6 - Absolute Position Block Denial of Service | windows/dos/[01;31m[K23[m[K215.html

Microsoft Internet Explorer 6 - Double Slash Cache Zone Bypass | windows/remote/[01;31m[K23[m[K340.txt

Microsoft Internet Explorer 6 - HTML Form Status Bar Misrepresentation | windows/remote/[01;31m[K23[m[K903.html

Microsoft Internet Explorer 6 - Local Resource Reference | windows/remote/[01;31m[K23[m[K283.txt

Microsoft Internet Explorer 6 - MSWebDVD Object Denial of Service | windows/dos/[01;31m[K23[m[K911.txt

Microsoft Internet Explorer 6 - Script Execution | windows/remote/[01;31m[K23[m[K131.txt

Microsoft Internet Explorer 6 - Scrollbar-Base-Color Partial Denial of Service | windows/dos/[01;31m[K23[m[K273.html

Microsoft Internet Explorer 6 - window.open Media Bar Cross-Zone Scripting | windows/remote/[01;31m[K23[m[K768.txt

Microsoft Internet Explorer 6 / Provideo Camimage - 'ISSCamControl.dll 1.0.1.5' Remote Buffer Overflow | windows/remote/40[01;31m[K23[m[K.html

Microsoft Internet Explorer 6 < 10 - Mouse Tracking | windows/remote/[01;31m[K23[m[K321.txt

Microsoft Internet Explorer 6.0 Macromedia Flash Player Plugin - Remote Denial of Service | windows/dos/[01;31m[K23[m[K912.txt

Microsoft Internet Explorer 6.x - IMG / XML elements Denial of Service | windows/dos/14[01;31m[K23[m[K.html

Microsoft Internet Explorer 7 - CSS Width Element Denial of Service | windows/dos/29[01;31m[K23[m[K6.html

Microsoft Internet Explorer 9 - IEFRAME CMarkup::RemovePointerPos Use-After-Free (MS13-055) | windows/dos/409[01;31m[K23[m[K.html

Microsoft Internet Explorer < 11 - OLE Automation Array Remote Code Execution (Metasploit) | windows/remote/35[01;31m[K23[m[K0.rb

Microsoft ListBox/ComboBox Control - 'User32.dll' Buffer Overrun | windows/local/[01;31m[K23[m[K255.cpp

Microsoft Office / COM Object - 'WMALFXGFXDSP.dll' DLL Planting (MS16-007) | windows/dos/39[01;31m[K23[m[K3.txt

Microsoft Office 2003 - '.PPT' Local Buffer Overflow (PoC) | windows/dos/25[01;31m[K23[m[K.pl

Microsoft Office 365 Version 18.[01;31m[K23[m[K05.1222.0 - Elevation of Privilege + RCE. | multiple/remote/51609.txt

Microsoft Office Picture Manager 2010 - Crash (PoC) | windows/dos/22[01;31m[K23[m[K7.txt

Microsoft OneNote (Version [01;31m[K23[m[K05 Build 16.0.16501.20074) 64-bit - Spoofing | multiple/remote/51538.txt

Microsoft Organization Chart 2 - Remote Code Execution | windows/remote/3[01;31m[K23[m[K39.txt

Microsoft Outlook 2002 - 'Mailto' Quoting Zone Bypass | windows/remote/[01;31m[K23[m[K796.html

Microsoft Outlook Express 6.0 - '.MHTML' Forced File Execution (1) | windows/remote/[01;31m[K23[m[K400.txt

Microsoft Outlook Express 6.0 - MHTML Forced File Execution (2) | windows/remote/[01;31m[K23[m[K401.txt

Microsoft Outlook Microsoft 365 MSO (Version [01;31m[K23[m[K06 Build 16.0.16529.20100) 32-bit - Remote Code Execution | multiple/remote/51574.txt

Microsoft PowerPoint 2010 - 'pptimpconv.dll' DLL Hijacking | windows/local/147[01;31m[K23[m[K.c

Microsoft Publisher 2010 - Crash (PoC) | windows/dos/2[01;31m[K23[m[K10.txt

Microsoft Remote Desktop 10.2.4(134) - Denial of Service (PoC) | macos/dos/46[01;31m[K23[m[K6.py

Microsoft SharePoint 2013 (Cloud) - Persistent Exception Handling (MS13-067) | windows/webapps/28[01;31m[K23[m[K8.txt

Microsoft SQL Server - Database Link Crawling Command Execution (Metasploit) | windows/remote/[01;31m[K23[m[K649.rb

Microsoft URLScan 2.5/RSA Security SecurID 5.0 - Configuration Enumeration | windows/remote/[01;31m[K23[m[K034.txt

Microsoft Visual Basic For Applications SDK 5.0/6.0/6.2/6.3 - Document Handling Buffer Overrun | windows/remote/[01;31m[K23[m[K094.txt

Microsoft VSCode Python Extension - Code Execution | multiple/local/48[01;31m[K23[m[K1.md

Microsoft Windows - '.LNK' Shortcut File Code Execution (Metasploit) | windows/local/4[01;31m[K23[m[K82.rb

Microsoft Windows - 'ATMFD.dll' CharString Stream Out-of-Bounds Reads (MS15-021) | windows/dos/379[01;31m[K23[m[K.txt

Microsoft Windows - 'nt!NtQueryInformationJobObject (information class 12)' Kernel Stack Memory Disclosure | windows/dos/42[01;31m[K23[m[K1.cpp

Microsoft Windows - 'nt!NtQueryInformationJobObject (information class 28)' Kernel Stack Memory Disclosure | windows/dos/42[01;31m[K23[m[K2.cpp

Microsoft Windows - 'nt!NtQueryInformationTransaction (information class 1)' Kernel Stack Memory Disclosur | windows/dos/42[01;31m[K23[m[K3.cpp

Microsoft Windows - 'USP10!CreateIndexTable' Uniscribe Font Processing Out-of-Bounds Memory Read | windows/dos/42[01;31m[K23[m[K7.txt

Microsoft Windows - 'USP10!MergeLigRecords' Uniscribe Font Processing Heap Memory Corruption | windows/dos/42[01;31m[K23[m[K4.txt

Microsoft Windows - 'USP10!NextCharInLiga' Uniscribe Font Processing Out-of-Bounds Memory Read | windows/dos/42[01;31m[K23[m[K8.txt

Microsoft Windows - 'USP10!otlSinglePosLookup::getCoverageTable' Uniscribe Font Processing Out-of-Bounds M | windows/dos/42[01;31m[K23[m[K9.txt

```
Microsoft Windows - 'USP10!SubstituteNtoM' Uniscribe Font Processing
Out-of-Bounds Memory Read             |
windows/dos/42[01;31m[K23[m[K6.txt

Microsoft Windows - 'USP10!ttoGetTableData' Uniscribe Font Processing
Out-of-Bounds Memory Read            |
windows/dos/42[01;31m[K23[m[K5.txt

Microsoft Windows - 'win32k!NtGdiExtGetObjectW' Kernel Stack Memory
Disclosure                            |
windows/dos/422[01;31m[K23[m[K.cpp

Microsoft Windows - 'win32k!NtGdiMakeFontDir' Kernel Stack Memory
Disclosure                            |
windows/dos/42[01;31m[K23[m[K0.txt

Microsoft Windows - AlwaysInstallElevated MSI (Metasploit)
| windows/local/[01;31m[K23[m[K007.rb

Microsoft Windows - CanonicalizePathName() Remote (MS06-040)
| windows/remote/22[01;31m[K23[m[K.c

Microsoft Windows - devenum.dll!DeviceMoniker::Load() Heap Corruption
Buffer Underflow (MS16-007)          |
windows/dos/39[01;31m[K23[m[K2.txt

Microsoft Windows - DFS Client Driver Arbitrary Drive Mapping Privilege
Escalation (MS16-1[01;31m[K23[m[K)             |
windows/local/40572.cs

Microsoft Windows - Image Acquisition Logger ActiveX Control Arbitrary
File Overwrite (1)                   |
windows/remote/3[01;31m[K23[m[K44.txt

Microsoft Windows - Image Acquisition Logger ActiveX Control Arbitrary
File Overwrite (2)                   |
windows/remote/3[01;31m[K23[m[K45.cpp

Microsoft Windows - NtUserGetClipboardAccessToken Token Leak (MS15-
0[01;31m[K23[m[K)                                    |
windows/local/38199.txt

Microsoft Windows - OLE Package Manager Code Execution (MS14-064)
(Metasploit)                          |
windows/local/35[01;31m[K23[m[K6.rb

Microsoft Windows - OLE Package Manager Code Execution (via Python)
(MS14-064) (Metasploit)               |
windows/local/35[01;31m[K23[m[K5.rb

Microsoft Windows - Workstation Service WKSSVC Remote (MS03-049)
| windows/remote/1[01;31m[K23[m[K.c
```

Microsoft Windows 11 [01;31m[K23[m[Kh2 - CLFS.sys Elevation of Privilege | windows/local/52270.c

Microsoft Windows 11 Pro [01;31m[K23[m[KH2 - Ancillary Function Driver for WinSock Privilege Escalation | windows/local/52284.C++

Microsoft Windows 11 Version 24H2 Cross Device Service - Elevation of Privilege | windows/local/5[01;31m[K23[m[K20.py

Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows/remote/4[01;31m[K23[m[K15.py

Microsoft Windows 98 - Fragmented UDP Flood Denial of Service | windows/dos/[01;31m[K23[m[K101.c

Microsoft Windows Help Program - 'WinHlp32.exe' Crash (PoC) | windows/dos/2[01;31m[K23[m[K03.pl

Microsoft Windows Kernel - 'IOCTL 0x120007 NsiGetParameter' nsiproxy/netio Pool Memory Disclosure | windows/dos/4[01;31m[K23[m[K38.cpp

Microsoft Windows Kernel - 'win32k.sys NtSetWindowLongPtr' Local Privilege Escalation (MS16-135) (1) | windows/local/408[01;31m[K23[m[K.txt

Microsoft Windows Kernel - Registry Hive Loading Relative Arbitrary Read in nt!RtlValidRelativeSecurityDes | windows/dos/40601.txt

Microsoft Windows Media Player 11.0.5721.5[01;31m[K23[m[K0 - Memory Corruption (PoC) | windows/dos/32477.py

Microsoft Windows NT 4.0/2000 - DLL Search Path | windows/local/20[01;31m[K23[m[K2.cpp

Microsoft Windows NT 4.0/2000 - Local Descriptor Table Privilege Escalation (MS04-011) | windows/local/[01;31m[K23[m[K989.c

Microsoft Windows NT 4.0/4.0 SP1/4.0 SP2/4.0 SP3 - Denial of Service Duplicate Hostname | windows/dos/19[01;31m[K23[m[K8.txt

Microsoft Windows NT/2000 - Terminal Server Service RDP Denial of Service | windows/dos/211[01;31m[K23[m[K.txt

Microsoft Windows Server 2000 - Help Facility '.CNT' File :Link Buffer Overflow |
windows/local/2[01;31m[K23[m[K54.c

Microsoft Windows Server 2000 - Subnet Bandwidth Manager RSVP Server Authority Hijacking |
windows/remote/[01;31m[K23[m[K019.c

Microsoft Windows Server 2003 - NetpIsRemote() Remote Overflow (MS06-040) (Metasploit) |
windows/remote/[01;31m[K23[m[K55.pm

Microsoft Windows Server 2016 - Win32k Elevation of Privilege
| windows/local/5[01;31m[K23[m[K01.c

Microsoft Windows Server 2025 JScript Engine - Remote Code Execution (RCE) |
windows/remote/5[01;31m[K23[m[K15.py

Microsoft Windows XP - 'explorer.exe' Remote Denial of Service
| windows/dos/[01;31m[K23[m[K850.txt

Microsoft Windows XP - HCP URI Buffer Overflow
| windows/dos/22[01;31m[K23[m[K2.txt

Microsoft Windows XP - HCP URI Handler Arbitrary Command Execution
| windows/remote/[01;31m[K23[m[K675.txt

Microsoft Windows XP - Help and Support Center Interface Spoofing
| windows/remote/[01;31m[K23[m[K717.txt

Microsoft Windows XP - TCP Packet Information Leakage
| windows/remote/[01;31m[K23[m[K093.txt

Microsoft Windows XP - Wireless Zero Configuration Service Information Disclosure |
windows/local/263[01;31m[K23[m[K.cpp

Microsoft Windows XP/2000 - Messenger Service Buffer Overrun (MS03-043)
| windows/remote/[01;31m[K23[m[K247.c

Microsoft Windows XP/2000 - PostThreadMessage() Arbitrary Process Killing |
windows/local/[01;31m[K23[m[K210.c

Microsoft Windows XP/2000 - showHelp '.CHM' File Execution (MS03-004)
| windows/dos/[01;31m[K23[m[K504.txt

Microsoft Windows XP/2000/2003 - 'win32k.sys' SfnINSTRING Local kernel Denial of Service | windows/dos/1[01;31m[K23[m[K37.c

Microsoft Windows XP/2000/2003 - 'win32k.sys' SfnLOGONNOTIFY Local kernel Denial of Service | windows/dos/1[01;31m[K23[m[K36.c

Microsoft Windows XP/2000/2003 - Graphical Device Interface Library Denial of Service | windows/dos/25[01;31m[K23[m[K1.txt

Microsoft Windows XP/2000/2003 - Message Queuing Service Heap Overflow | windows/remote/[01;31m[K23[m[K229.cpp

Microsoft Windows XP/2000/NT 4.0 - NetDDE Privilege Escalation (2) | windows/local/219[01;31m[K23[m[K.c

Microsoft Word 16.72.[01;31m[K23[m[K040900 - Remote Code Execution (RCE) | multiple/remote/51376.txt

Microsoft Word 2013/2016 - sprmSdyaTop Denial of Service (MS16-099) | multiple/dos/40[01;31m[K23[m[K8.txt

Microsoft Word 97/98/2002 - Malformed Document Denial of Service | windows/dos/[01;31m[K23[m[K216.txt

Microsoft Wordpad on winXP SP3 - Local Crash | windows/dos/94[01;31m[K23[m[K.pl

Microsoft WordPerfect - Converter Buffer Overrun | windows/local/[01;31m[K23[m[K096.txt

Mida eFramework 2.9.0 - Back Door Access | hardware/webapps/488[01;31m[K23[m[K.py

MilleGPG5 5.9.2 (Gennaio 20[01;31m[K23[m[K) - Local Privilege Escalation / Incorrect Access Control | windows/local/51410.txt

Minerva 2.0.21 build [01;31m[K23[m[K8a - 'phpbb_root_path' File Inclusion | php/webapps/2429.txt

Minerva 2.0.8a Build [01;31m[K23[m[K7 - 'phpbb_root_path' File Inclusion | php/webapps/1908.txt

MiniBB RSS 2.0 Plugin - Multiple Remote File Inclusions | php/webapps/321[01;31m[K23[m[K.txt

minihttp file-sharing for net 1.5 - Directory Traversal | windows/remote/[01;31m[K23[m[K144.txt

MiniPort@l 0.1.5 Beta - 'skiny' Remote File Inclusion | php/webapps/[01;31m[K23[m[K43.py

Miniweb 0.8.19 - Multiple Vulnerabilities
| windows/remote/49[01;31m[K23[m[K.txt

MiniWeb 0.8.19 - Remote Buffer Overflow
| windows/remote/329[01;31m[K23[m[K.cs

mIRC 6.1 - 'DCC SEND' Buffer Overflow (1)
| windows/dos/[01;31m[K23[m[K240.pl

mIRC 6.1 - 'DCC SEND' Buffer Overflow (2)
| windows/dos/[01;31m[K23[m[K241.pl

mIRC 6.1 - DCC Get Dialog Denial of Service
| windows/dos/[01;31m[K23[m[K602.txt

Mitsubishi Electric & INEA SmartRTU - Reflected Cross-Site Scripting
(XSS) |
hardware/webapps/504[01;31m[K23[m[K.txt

Mitsubishi Electric smartRTU / INEA ME-RTU - Unauthenticated
Configuration Download |
php/webapps/47[01;31m[K23[m[K4.py

Mitsubishi Electric smartRTU / INEA ME-RTU - Unauthenticated OS Command
Injection Bind Shell | php/webapps/47[01;31m[K23[m[K5.py

Miyabi CGI Tools 1.02 - 'index.pl' Remote Command Execution
| cgi/webapps/342[01;31m[K23[m[K.txt

MJM Core Player 2011 - '.s3m' Local Stack Buffer Overflow (Metasploit)
| windows/local/17[01;31m[K23[m[K0.rb

ml2 - Local users can Crash processes
| linux/dos/[01;31m[K23[m[K8.c

MLdonkey 2.5-4 - Cross-Site Scripting
| multiple/remote/[01;31m[K23[m[K320.txt

mlsrvx.dll 1.8.9.1 ArGoSoft Mail Server - Data Write/Code Execution
| windows/remote/4[01;31m[K23[m[K4.html

Moa Gallery 1.2.0 - 'index.php?action' SQL Injection
| php/webapps/95[01;31m[K23[m[K.txt

MobilePublisherPHP 1.5 RC2 - Remote File Inclusion
| php/webapps/[01;31m[K23[m[K83.txt

modifyform - 'modifyform.html' Remote File Inclusion
| php/webapps/44[01;31m[K23[m[K.txt

Mongoose Web Server 2.8 - Multiple Directory Traversals
| windows/remote/1[01;31m[K23[m[K09.txt

```
Monit 1.4/2.x/3/4 - 'HTTP Request' Buffer Overrun
| linux/remote/[01;31m[K23[m[K397.pl

Monkey HTTP Daemon 0.x - Missing Host Field Denial of Service
| windows/dos/[01;31m[K23[m[K686.txt

Mono 2.0 - 'System.Web' HTTP Header Injection
| linux/remote/3[01;31m[K23[m[K03.txt

more.groupware 0.74 - 'new_calendarid' SQL Injection
| php/webapps/[01;31m[K23[m[K94.php

Motorola T720 Phone - Denial of Service
| hardware/dos/[01;31m[K23[m[K778.c

Motorola Timbuktu Pro 8.6.5/8.7 - Directory Traversal / Log Injection
| windows/remote/5[01;31m[K23[m[K8.py

Mozilla Browser 1.5 - URI MouseOver Obfuscation
| multiple/remote/[01;31m[K23[m[K433.txt

Mozilla Firefox 1.0.7 - Integer Overflow Denial of Service
| multiple/dos/1[01;31m[K23[m[K3.html

Mozilla Firefox 2.0.0.2 - '.GIF' Handling Denial of Service
| linux/dos/297[01;31m[K23[m[K.txt

Mozilla Thunderbird 17.0.6 - Input Validation Filter Bypass
| multiple/dos/312[01;31m[K23[m[K.txt

Mozilla Thunderbird 2.0.0.[01;31m[K23[m[K Mozilla SeaMonkey 2.0 -
'jar50.dll' Null Pointer Dereference                  |
windows/dos/10103.txt

MP3Info 0.8.5a - Local Buffer Overflow (SEH)
| windows/local/3[01;31m[K23[m[K58.pl

MPG1[01;31m[K23[m[K 0.59 - Find Next File Remote Client-Side Buffer
Overflow                                              |
linux/remote/24852.txt

MPG1[01;31m[K23[m[K 0.59 - Remote File Play Heap Corruption
| linux/remote/[01;31m[K23[m[K171.c

mpg1[01;31m[K23[m[K 0.59r - Malformed .mp3 (SIGSEGV) (PoC)
| linux/dos/1634.pl

mpg1[01;31m[K23[m[K pre0.59s - Invalid MP3 Header Memory Corruption
| linux/remote/22147.c

MPlayer 0.9/1.0 - Remote HTTP Header Buffer Overflow
| linux/dos/[01;31m[K23[m[K896.txt
```

```
MPlayer 0.9/1.0 - Streaming ASX Header Parsing Buffer Overrun
| linux/remote/[01;31m[K23[m[K186.txt

MPM Guestbook 1.2 - Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K332.txt

mpnews pro 2.1.0.18 - Directory Traversal Information Disclosure
| php/webapps/[01;31m[K23[m[K208.txt

MTools 3.9.x - 'MFormat' Local Privilege Escalation
| linux/local/[01;31m[K23[m[K759.pl

Multi-Mirror - Arbitrary File Upload
| php/webapps/122[01;31m[K23[m[K.txt

Multi-Threaded HTTP Server 1.1 - Directory Traversal (1)
| multiple/remote/1[01;31m[K23[m[K04.txt

Multi-Threaded HTTP Server 1.1 - Directory Traversal (2)
| windows/remote/1[01;31m[K23[m[K31.txt

Multi-Threaded HTTP Server 1.1 - Source Disclosure
| windows/remote/1[01;31m[K23[m[K08.txt

Multi-Threaded TFTP 1.1 - GET Denial of Service
| windows/dos/[01;31m[K23[m[K34.py

Multiple Browsers - Audio Tag Denial of Service
| multiple/dos/1[01;31m[K23[m[K24.py

Multiple Vendor FTP Server - Long Command Handling Security
| unix/remote/3[01;31m[K23[m[K99.txt

Multitech RouteFinder 550 - Remote Memory Corruption
| multiple/dos/2[01;31m[K23[m[K45.txt

MultiTheftAuto 0.5 patch 1 - Server Crash / MOTD Deletion
| windows/dos/1[01;31m[K23[m[K5.c

MuPDF < 20091125[01;31m[K23[m[K1942 - 'pdf_shade4.c' Multiple Stack
Buffer Overflows                                        |
windows/local/10244.txt

MusicBox - SQL Injection
| php/webapps/128[01;31m[K23[m[K.txt

MusicBox 3.3 - SQL Injection
| php/webapps/1[01;31m[K23[m[K03.pl

Musicqueue 0.9/1.0/1.1 - Multiple Buffer Overrun Vulnerabilities
| linux/local/[01;31m[K23[m[K303.c
```

```
Musicqueue 1.2 - SIGSEGV Signal Handler Insecure File Creation
| linux/local/[01;31m[K23[m[K297.c

mutant penguin mpweb pro 1.1.2 - Directory Traversal
| windows/remote/[01;31m[K23[m[K209.txt

MVDSV 0.165 b/0.171 Quake Server - Download Buffer Overrun
| multiple/remote/[01;31m[K23[m[K439.txt

mxBB Module mx_blogs 2.0.0-beta - Remote File Inclusion
| php/webapps/53[01;31m[K23[m[K.pl

My Blog 1.63 - BBCode HTML Injection
| php/webapps/27[01;31m[K23[m[K0.txt

My Little Forum 1.3 - 'email.php' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K473.txt

MyABraCaDaWeb 1.0 - Full Path Disclosure
| php/webapps/2[01;31m[K23[m[K78.txt

MyABraCaDaWeb 1.0.3 - 'base' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K35.txt

MyBB 1.0.3 - 'private.php' Multiple SQL Injections
| php/webapps/27[01;31m[K23[m[K6.txt

MyBB 1.4.8 - 'search.php' SQL Injection
| php/webapps/33[01;31m[K23[m[K2.txt

MyBB 1.6.9 - 'editpost.php?posthash' Blind SQL Injection
| php/webapps/[01;31m[K23[m[K781.txt

MyBB 1.8.2 - 'unset_globals()' Function Bypass / Remote Code Execution
| php/webapps/353[01;31m[K23[m[K.md

MyBB AJAX Chat - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K354.txt

MyBB AwayList Plugin - 'index.php?id' SQL Injection
| php/webapps/[01;31m[K23[m[K625.txt

MyBB Bank- 3 Plugin - SQL Injection
| php/webapps/[01;31m[K23[m[K284.txt

MyBB DyMy User Agent Plugin - 'newreply.php' SQL Injection
| php/webapps/[01;31m[K23[m[K359.txt

MyBB HM My Country Flags - SQL Injection
| php/webapps/[01;31m[K23[m[K624.txt

MyBB KingChat Plugin - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K249.txt
```

MyBB KingChat Plugin - SQL Injection
| php/webapps/[01;31m[K23[m[K105.txt

MyBB Profile Blogs Plugin 1.2 - Multiple Vulnerabilities
| php/webapps/[01;31m[K23[m[K287.txt

MyBB Profile Wii Friend Code - Multiple Vulnerabilities
| php/webapps/[01;31m[K23[m[K888.txt

MyBB User Profile Skype ID Plugin 1.0 - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K425.txt

MyBlog 1.x - 'Games.php?ID' Remote File Inclusion
| php/webapps/309[01;31m[K23[m[K.txt

MyBloggie 2.1.1 < 2.1.2 - SQL Injection
| php/webapps/10[01;31m[K23[m[K.pl

MyNews 0.10 - AuthACC SQL Injection
| php/webapps/30[01;31m[K23[m[K0.txt

myPHPNuke 1.8.8 - 'auth.inc.php' SQL Injection
| php/webapps/[01;31m[K23[m[K164.txt

MyReview 1.9.4 - 'email' SQL Injection / Code Execution
| php/webapps/[01;31m[K23[m[K97.py

myServer 0.4.x - 'cgi-lib.dll' Remote Buffer Overflow (PoC)
| windows/dos/[01;31m[K23[m[K139.txt

MySpeach 3.0.2 - 'my_ms[root]' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K01.txt

MySQL (Linux) - Database Privilege Escalation
| linux/local/[01;31m[K23[m[K077.pl

MySQL (Linux) - Heap Overrun (PoC)
| linux/dos/[01;31m[K23[m[K076.pl

MySQL (Linux) - Stack Buffer Overrun (PoC)
| linux/dos/[01;31m[K23[m[K075.pl

MySQL - 'Stuxnet Technique' Windows Remote System
| windows/remote/[01;31m[K23[m[K083.txt

MySQL - Denial of Service (PoC)
| linux/dos/[01;31m[K23[m[K078.txt

MySQL - Remote User Enumeration
| multiple/remote/[01;31m[K23[m[K081.pl

MySQL 3.20.32 a/3.[01;31m[K23[m[K.34 - Root Operation Symbolic Link File Overwriting | unix/local/20718.txt

MySQL 3.20.32/3.22.x/3.[01;31m[K23[m[K.x - Null Root Password Weak Default Configuration (1) | linux/remote/21725.c

MySQL 3.20.32/3.22.x/3.[01;31m[K23[m[K.x - Null Root Password Weak Default Configuration (2) | linux/remote/21726.c

MySQL 3.22.27/3.22.29/3.[01;31m[K23[m[K.8 - GRANT Global Password Changing | multiple/local/19721.txt

Mysql 3.22.x/3.[01;31m[K23[m[K.x - Local Buffer Overflow | linux/local/20581.c

MySQL 3.[01;31m[K23[m[K.x - 'mysqld' Local Privilege Escalation | linux/local/2[01;31m[K23[m[K40.txt

MySQL 3.[01;31m[K23[m[K.x/4.0.x - 'COM_CHANGE_USER' Password Length Account | unix/remote/22084.c

MySQL 3.[01;31m[K23[m[K.x/4.0.x - COM_CHANGE_USER Password Memory Corruption | unix/remote/22085.txt

MySQL 3.[01;31m[K23[m[K.x/4.0.x - Password Handler Buffer Overflow | linux/dos/[01;31m[K23[m[K138.txt

MySQL 3.[01;31m[K23[m[K.x/4.0.x - Remote Buffer Overflow | linux/remote/98.c

MySQL 4.x/5.x - Server Date_Format Denial of Service | linux/dos/28[01;31m[K23[m[K4.txt

MySQL 5.1.[01;31m[K23[m[K - Server InnoDB CONVERT_SEARCH_MODE_TO_INNOBASE Function Denial of Service | linux/dos/30744.txt

MySQL 5.1/5.5 (Windows) - 'MySQLJackpot' Remote Command Execution | windows/remote/[01;31m[K23[m[K073.txt

MySQL 6.0.4 - Empty Binary String Literal Remote Denial of Service | linux/dos/3[01;31m[K23[m[K48.txt

MySQL MaxDB Webtool 7.5.00.[01;31m[K23[m[K - Remote Stack Overflow | windows/remote/960.c

MySQL User-Defined (Linux) x32 / x86_64 - 'sys_exec' Local Privilege Escalation (2) | linux/local/50[01;31m[K23[m[K6.py

Mythic Entertainment Dark Age of Camelot 1.6x - Encryption Key Signing | multiple/remote/[01;31m[K23[m[K873.c

MyYoutube MyBB Plugin 1.0 - SQL Injection | php/webapps/[01;31m[K23[m[K353.txt

My_eGallery Module 3.1.1 - Remote File Inclusion Command Injection | php/webapps/[01;31m[K23[m[K403.pl

Nadeo Game Engine - Remote Denial of Service | linux/dos/[01;31m[K23[m[K662.c

Nagios XI - 'users.php' SQL Injection | multiple/remote/345[01;31m[K23[m[K.txt

Nagios XI Network Monitor Graph Explorer Component - Command Injection (Metasploit) | unix/remote/[01;31m[K23[m[K227.rb

Nanometrics Centaur 4.3.[01;31m[K23[m[K - Unauthenticated Remote Memory Leak | hardware/webapps/48098.py

NCSA httpd-campas 1.2 - sample script | cgi/remote/204[01;31m[K23[m[K.txt

NCT Jobs Portal Script - Cross-Site Scripting / Authentication Bypass | php/webapps/1[01;31m[K23[m[K70.txt

ncube server manager 1.0 - Directory Traversal | cgi/webapps/[01;31m[K23[m[K370.txt

NEC UNIVERGE UM4730 < 11.8 - SQL Injection | php/webapps/4[01;31m[K23[m[K53.txt

Neon WebDAV Client Library 0.2x - Format String | linux/dos/[01;31m[K23[m[K999.txt

Nessus Vulnerability Scanner 3.0.6 - ActiveX Command Execution | windows/remote/4[01;31m[K23[m[K7.html

Nessus Vulnerability Scanner 3.0.6 - ActiveX Remote Delete File | windows/remote/4[01;31m[K23[m[K0.html

Netbula Anyboard 9.9.5 6 - Information Disclosure | cgi/webapps/[01;31m[K23[m[K059.txt

Netbus 2.0 Pro - Directory Listings Disclosure / Arbitrary File Upload | multiple/remote/[01;31m[K23[m[K583.txt

NetCat CMS - Multiple Vulnerabilities
| php/webapps/178[01;31m[K23[m[K.txt

NetClassifieds 1.9.7 - Multiple Input Validation Vulnerabilities
| php/webapps/302[01;31m[K23[m[K.txt

NetcPlus BrowseGate 2.80 - Denial of Service
| windows/dos/20[01;31m[K23[m[K3.txt

NETGATE AMITI Antivirus [01;31m[K23[m[K.0.305 - Unquoted Service Path
Privilege Escalation |
windows/local/40540.txt

Netgear FM114P Wireless Firewall - File Disclosure
| hardware/remote/22[01;31m[K23[m[K6.txt

Netgear Voice Gateway 2.3.0.[01;31m[K23[m[K_2.3.[01;31m[K23[m[K -
Multiple Vulnerabilities |
hardware/webapps/38449.txt

Netgear Wireless Management System 2.1.4.15 (Build 1[01;31m[K23[m[K6) -
Privilege Escalation |
hardware/webapps/38097.txt

Nethack 3 - Local Buffer Overflow (1)
| linux/local/22[01;31m[K23[m[K3.c

Nethack 3 - Local Buffer Overflow (2)
| linux/local/22[01;31m[K23[m[K4.c

Nethack 3 - Local Buffer Overflow (3)
| linux/local/22[01;31m[K23[m[K5.pl

Netis WF2419 2.2.361[01;31m[K23[m[K - Remote Code Execution
| hardware/webapps/48149.py

NetNote Server 2.2 build [01;31m[K23[m[K0 - Crafted String Denial of
Service | windows/dos/628.c

NETObserve 2.0 - Authentication Bypass
| windows/remote/[01;31m[K23[m[K503.txt

NetOp Remote Control 8.0/9.1/9.2/9.5 - Local Buffer Overflow
| windows/local/172[01;31m[K23[m[K.pl

Netopia Timbuktu Pro for Macintosh 6.0.1 - Denial of Service
| osx/dos/21[01;31m[K23[m[K4.sh

Netscaler SD-WAN 9.1.2.26.561201 - Command Injection (Metasploit)
| cgi/webapps/4[01;31m[K23[m[K45.rb

Netscape Enterprise Server 4.1 - HTTP Method Name Buffer Overflow
| multiple/dos/22[01;31m[K23[m[K0.pl

```
Netscape Messaging Server 3.55 & University of Washington imapd
10.[01;31m[K23[m[K4 - Remote Buffer Overflow            |
linux/remote/19107.c

netserve Web server 1.0.7 - Directory Traversal
| windows/remote/[01;31m[K23[m[K387.txt

NetSupport School 7.0/7.5 - Weak Password Encryption
| linux/local/[01;31m[K23[m[K882.pas

Netwave IP Camera - Password Disclosure
| hardware/remote/41[01;31m[K23[m[K6.py

NetWin DBabble 2.5 i - Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K153.txt

NetWin SurgeFTP - (Authenticated) Admin Command Injection (Metasploit)
| multiple/remote/[01;31m[K23[m[K522.rb

Netwin SurgeFTP - Remote Command Execution (Metasploit)
| multiple/remote/[01;31m[K23[m[K601.rb

Netwin SurgeFTP Sever [01;31m[K23[m[Kd6 - Persistent Cross-Site
Scripting                                               |
windows/webapps/38762.txt

Network Associates PGP KeyServer 7 - LDAP Buffer Overflow (Metasploit)
| windows/remote/168[01;31m[K23[m[K.rb

Network Shutdown Module 3.21 - 'sort_values' Remote PHP Code Injection
(Metasploit)                        | php/remote/[01;31m[K23[m[K006.rb

News Evolution 3.0.3 - _NE[AbsPath] Remote File Inclusion
| php/webapps/[01;31m[K23[m[K25.txt

News Wizard 2.0 - Full Path Disclosure
| php/webapps/[01;31m[K23[m[K012.txt

newsPHP 216 - Authentication Bypass
| php/webapps/[01;31m[K23[m[K058.txt

newsPHP 216 - Remote File Inclusion
| php/webapps/[01;31m[K23[m[K057.txt

Newsscript 0.5 - Local/Remote File Inclusion
| php/webapps/[01;31m[K23[m[K65.txt

NexGen FTP Server 1.0/2.x - Directory Traversal
| windows/remote/[01;31m[K23[m[K877.txt

Nexpose Security Console - Cross-Site Request Forgery
| multiple/webapps/[01;31m[K23[m[K924.txt
```

```
NfSen < 1.3.7 / AlienVault OSSIM 4.3.1 - 'customfmt' Command Injection
| linux/webapps/4[01;31m[K23[m[K14.txt

NfSen < 1.3.7 / AlienVault OSSIM 5.3.4 - Command Injection
| linux/webapps/4[01;31m[K23[m[K06.txt

NfSen < 1.3.7 / AlienVault OSSIM < 5.3.6 - Local Privilege Escalation
| linux/local/4[01;31m[K23[m[K05.txt

Niti Telecom Caravan Business Server 2.00-03D - Directory Traversal
| asp/webapps/[01;31m[K23[m[K635.txt

NKINFOWEB - SQL Injection
| php/webapps/1[01;31m[K23[m[K54.pl

NodCMS - PHP Code Execution
| php/webapps/407[01;31m[K23[m[K.txt

Nokia Electronic Documentation 5.0 - Connection redirection
| windows/remote/[01;31m[K23[m[K148.txt

Nokia Electronic Documentation 5.0 - Cross-Site Scripting
| windows/remote/[01;31m[K23[m[K149.txt

Nokia Electronic Documentation 5.0 - Path Disclosure
| windows/remote/[01;31m[K23[m[K147.txt

Nokia N70 - L2CAP Packets Remote Denial of Service
| hardware/dos/27[01;31m[K23[m[K2.txt

Nokia SGSN DX200 - Remote SNMP Information Disclosure
| hardware/remote/2[01;31m[K23[m[K50.txt

Nooms 1.1 - 'search.php?q' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K61.txt

Nooms 1.1 - 'smileys.php?page_id' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K60.txt

Nortel Wireless LAN Access Point 2200 Series - Denial of Service
| hardware/dos/[01;31m[K23[m[K786.c

Norton Ghost Support module for EasySetup wizard - Remote Denial of
Service (PoC)                          |
windows/dos/85[01;31m[K23[m[K.txt

Novatel Wireless MiFi [01;31m[K23[m[K52 - Password Information
Disclosure                                                  |
hardware/remote/33568.txt

Novell eDirectory 8 - Remote Buffer Overflow (Metasploit)
| multiple/remote/243[01;31m[K23[m[K.rb
```

Novell File Reporter (NFR) Agent - XML Parsing Remote Code Execution
| windows/remote/[01;31m[K23[m[K3[01;31m[K23[m[K.py

Novell iPrint Client - ActiveX Control target-frame Buffer Overflow
(Metasploit) |
windows/remote/165[01;31m[K23[m[K.rb

Novell Netware - RPC XNFS xdrDecodeString
| netware/dos/16[01;31m[K23[m[K4.rb

Novell Netware Enterprise Web Server 5.1/6.0 - env.bas Information
Disclosure |
netware/remote/[01;31m[K23[m[K586.txt

Novell Netware Enterprise Web Server 5.1/6.0 - Multiple Cross-Site
Scripting Vulnerabilities |
netware/remote/[01;31m[K23[m[K589.txt

Novell Netware Enterprise Web Server 5.1/6.0 - snoop.jsp Information
Disclosure |
netware/remote/[01;31m[K23[m[K587.txt

Novell Netware Enterprise Web Server 5.1/6.0 SnoopServlet - Information
Disclosure |
netware/remote/[01;31m[K23[m[K588.txt

NSTX 1.0/1.1 - Remote Denial of Service
| linux/dos/[01;31m[K23[m[K884.txt

NukeCalendar 1.1.a - 'block-calendar.php' Full Path Disclosure
| php/webapps/[01;31m[K23[m[K929.txt

NukeCalendar 1.1.a - 'block-Calendar1.php' Full Path Disclosure
| php/webapps/[01;31m[K23[m[K930.txt

NukeCalendar 1.1.a - 'block-Calendar_center.php' Full Path Disclosure
| php/webapps/[01;31m[K23[m[K931.txt

NukeCalendar 1.1.a - 'eid' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K932.txt

NukeCalendar 1.1.a - 'eid' SQL Injection
| php/webapps/[01;31m[K23[m[K933.txt

NukeCalendar 1.1.a - 'modules.php' Full Path Disclosure
| php/webapps/[01;31m[K23[m[K928.txt

Nuked-klaN 1.x - Multiple Vulnerabilities
| php/webapps/[01;31m[K23[m[K988.txt

NullLogic Null HTTPd 0.5 - Remote Denial of Service
| multiple/dos/[01;31m[K23[m[K181.txt

NullLogic Null HTTPd 0.5.1 - Error Page Long HTTP Request Cross-Site Scripting |
multiple/remote/[01;31m[K23[m[K176.txt

Nullsoft SHOUTcast 1.9.2 - 'icy-name/icy-url' Memory Corruption (1)
| windows/remote/[01;31m[K23[m[K328.py

Nullsoft SHOUTcast 1.9.2 - 'icy-name/icy-url' Memory Corruption (2)
| windows/remote/[01;31m[K23[m[K329.c

NullSoft Winamp 2.81/2.91/3.0/3.1 - MIDI Plugin 'IN_MIDI.dll' Track Data Size Buffer Overflow (PoC) |
windows/dos/[01;31m[K23[m[K124.txt

Nvidia Install Application 2.1002.85.551 - 'NVI2.dll' Unicode Buffer Overflow (PoC) |
windows/dos/[01;31m[K23[m[K177.txt

NVR SP2 2.0 'nvUtility.dll 1.0.14.0' - 'SaveXMLFile()' Insecure Method
| windows/remote/43[01;31m[K23[m[K.html

Online Admission System 1.0 - Remote Code Execution (RCE) (Unauthenticated) |
php/webapps/506[01;31m[K23[m[K.py

Online Quiz Maker 1.0 - 'catid' SQL Injection
| php/webapps/453[01;31m[K23[m[K.txt

Online Shopping Cart System 1.0 - 'id' SQL Injection
| php/webapps/494[01;31m[K23[m[K.txt

OnlineArts DailyDose 1.1 - 'dose.pl' Remote Command Execution
| cgi/webapps/[01;31m[K23[m[K367.txt

Open Bulletin Board 1.0.8 - 'ROOT_PATH' File Inclusion
| php/webapps/[01;31m[K23[m[K41.txt

OpenAutoClassifieds 1.0 - 'Listing' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K336.txt

OpenBB 1.0 - 'board.php' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K483.txt

OpenBB 1.0.6 - 'myhome.php' SQL Injection
| php/webapps/[01;31m[K23[m[K908.txt

OpenBSD 2.x/3.x - Local Malformed Binary Execution Denial of Service
| openbsd/dos/[01;31m[K23[m[K339.c

OpenBSD 3.3 - 'Semget()' Integer Overflow (1)
| openbsd/local/[01;31m[K23[m[K046.c

OpenBSD 3.3 - 'Semget()' Integer Overflow (2)
| openbsd/local/[01;31m[K23[m[K047.c

OpenBSD 3.3/3.4 - 'sysctl' Local Denial of Service
| openbsd/dos/[01;31m[K23[m[K389.c

OpenBSD 3.3/3.4 - semctl/semop Local Unexpected Array Indexing
| openbsd/dos/[01;31m[K23[m[K392.c

OpenBSD ftpd 2.6/2.7 - Remote Overflow
| bsd/remote/[01;31m[K23[m[K4.c

OpenCominterne 1.01 - Local File Inclusion
| php/webapps/1[01;31m[K23[m[K96.txt

Opencourrier 2.03beta - Local File Inclusion / Remote File Inclusion
| php/webapps/1[01;31m[K23[m[K98.txt

OpenDB 1.0.6 - 'listings.php?title' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K14.txt

OpenDB 1.0.6 - 'user_admin.php?user_id' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K13.txt

OpenDB 1.0.6 - 'user_profile.php?redirect_url' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K15.txt

OpenEMR 5.0.0 - OS Command Injection / Cross-Site Scripting
| php/webapps/43[01;31m[K23[m[K2.txt

OpenEMR 5.0.1 - 'controller' Remote Code Execution
| php/webapps/486[01;31m[K23[m[K.txt

openEngine 1.7/1.8 - Template Unauthorized Access
| php/webapps/278[01;31m[K23[m[K.txt

Openfire 4.6.0 - 'groupchatJID' Stored XSS
| jsp/webapps/49[01;31m[K23[m[K3.txt

Openfire 4.6.0 - 'sql' Stored XSS
| jsp/webapps/49[01;31m[K23[m[K5.txt

Openfire 4.6.0 - 'users' Stored XSS
| jsp/webapps/49[01;31m[K23[m[K4.txt

Openfoncier 2.00 - Local File Inclusion / Remote File Inclusion
| php/webapps/1[01;31m[K23[m[K66.txt

OpenH3[01;31m[K23[m[K Opal SIP Protocol - Remote Denial of Service
| windows/dos/9240.py

OPENi-CMS 1.0.1beta - 'config' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K44.txt

```
OpenJournal 2.0 - Authentication Bypassing
| cgi/webapps/[01;31m[K23[m[K659.txt

OpenMediaVault Cron - Remote Command Execution (Metasploit)
| linux/remote/293[01;31m[K23[m[K.rb

openmovieeditor 0.0.20060901 - 'name' Local Buffer Overflow
| linux/local/[01;31m[K23[m[K38.c

OpenNMS 1.5.x - 'j_username' Cross-Site Scripting
| jsp/webapps/324[01;31m[K23[m[K.txt

OpenOffice - OLE Importer DocumentSummaryInformation Stream Handling
Overflow (Metasploit)                  |
windows/local/189[01;31m[K23[m[K.rb

OpenOffice 1.0.1 - Remote Access Denial of Service
| windows/dos/[01;31m[K23[m[K[01;31m[K23[m[K5.txt

Openplanning 1.00 - Local File Inclusion / Remote File Inclusion
| php/webapps/1[01;31m[K23[m[K65.txt

Openpresse 1.01 - Local File Inclusion
| php/webapps/1[01;31m[K23[m[K64.txt

Openregistrecil 1.02 - Local File Inclusion / Remote File Inclusion
| php/webapps/1[01;31m[K23[m[K13.txt

OpenSSH 2.3 < 7.7 - Username Enumeration
| linux/remote/45[01;31m[K23[m[K3.py

OpenSSL - ASN.1 Parsing
| multiple/remote/[01;31m[K23[m[K199.c

OpenSSL - Remote Denial of Service
| linux/dos/1[01;31m[K23[m[K34.c

OpenSupports 2.0 - Blind SQL Injection
| php/webapps/3[01;31m[K23[m[K30.txt

OpenSupports 2.x - Authentication Bypass / Cross-Site Request Forgery
| php/webapps/3[01;31m[K23[m[K19.txt

Opera 6.0/7.0 - 'Filename Download' Buffer Overrun
| windows/remote/2[01;31m[K23[m[K41.txt

Opera 6.0/7.0 - 'Username' URI Warning Dialog Buffer Overflow
| windows/dos/22[01;31m[K23[m[K9.txt

Opera 7.11/7.20 HREF - Malformed Server Name Heap Corruption
| multiple/dos/[01;31m[K23[m[K263.txt
```

Opera 7.x - Directory Traversal
| windows/remote/[01;31m[K23[m[K464.pl

Opera Browser 6.0 6 - URI Display Obfuscation
| windows/remote/[01;31m[K23[m[K465.txt

Opera Web Browser 12.11 - Crash (PoC)
| windows/dos/[01;31m[K23[m[K107.txt

Opera Web Browser 7 - IFRAME Zone Restriction Bypass
| multiple/remote/[01;31m[K23[m[K291.txt

Opera Web Browser 7.0 - Remote IFRAME Denial of Service
| windows/dos/[01;31m[K23[m[K927.txt

Opera Web Browser 7.[01;31m[K23[m[K - Empty Embedded Object JavaScript
Denial of Service |
windows/dos/24426.html

Opera Web Browser 7.[01;31m[K23[m[K - JavaScript Denial of Service
| multiple/dos/24394.txt

Opera Web Browser 7.x - URI Handler Directory Traversal
| windows/remote/[01;31m[K23[m[K373.html

OptiSoft Blubster 2.5 - Remote Denial of Service
| windows/dos/[01;31m[K23[m[K056.c

Oracle 8i - 'dbsnmp' Remote Denial of Service
| multiple/dos/21[01;31m[K23[m[K2.c

Oracle 9.x - 'Database' / Statement Buffer Overflow
| multiple/dos/[01;31m[K23[m[K656.txt

Oracle Database Server 9.0.x - Oracle Binary Local Buffer Overflow
| linux/local/[01;31m[K23[m[K258.c

Oracle E-Business Suite 12.x - Server-Side Request Forgery
| jsp/webapps/4[01;31m[K23[m[K40.txt

Oracle HTTP Server 8.1.7/9.0.1/9.2 - isqlplus Cross-Site Scripting
| multiple/remote/[01;31m[K23[m[K593.txt

Oracle Java Runtime Environment - Heap Corruption During TTF font
Rendering in GlyphIterator::setCurrGlyph |
multiple/dos/467[01;31m[K23[m[K.txt

Oracle MySQL (Windows) - MOF Execution (Metasploit)
| windows/remote/[01;31m[K23[m[K179.rb

Oracle OpenSSO 8.0 - Multiple Cross-Site Scripting POST Injection
Vulnerabilities |
multiple/webapps/[01;31m[K23[m[K004.txt

```
OracleAS TopLink Mapping Workbench - Weak Encryption Algorithm
| multiple/local/[01;31m[K23[m[K611.pl

OrangeHRM 2.6.0.1 - Local File Inclusion
| php/webapps/15[01;31m[K23[m[K2.txt

Orangescrum 1.6.1 - Multiple Vulnerabilities
| php/webapps/4[01;31m[K23[m[K30.txt

osCommerce 2.1/2.2 - 'Checkout_Payment.php' Error Output Cross-Site
Scripting                                |
php/webapps/2[01;31m[K23[m[K93.txt

osCommerce 2.1/2.2 - Error_Message Cross-Site Scripting
| php/webapps/2[01;31m[K23[m[K91.txt

osCommerce 2.1/2.2 - Info_Message Cross-Site Scripting
| php/webapps/2[01;31m[K23[m[K92.txt

osCommerce 2.2 - 'manufacturers_id' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K463.txt

osCommerce 2.2 - 'osCsid' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K445.txt

osCommerce 2.2 - 'products_id' SQL Injection
| php/webapps/[01;31m[K23[m[K462.txt

osCommerce 2.2 - SQL Injection
| php/webapps/[01;31m[K23[m[K434.pl

OSSEC 2.8 - 'hosts.deny' Local Privilege Escalation
| linux/local/35[01;31m[K23[m[K4.py

Outblaze Webmail - Cookie Authentication Bypass
| cgi/webapps/2[01;31m[K23[m[K64.c

Ovidentia 6.6.5 - 'item' SQL Injection
| php/webapps/6[01;31m[K23[m[K2.txt

OXID eShop < 4.7.11/5.0.11 / < 4.8.4/5.1.4 - Multiple Vulnerabilities
| php/webapps/3[01;31m[K23[m[K75.txt

p4CMS 1.05 - 'abs_pfad' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K50.txt

Paid Memberships Pro  v2.9.8 (WordPress Plugin) - Unauthenticated SQL
Injection                              |
php/webapps/51[01;31m[K23[m[K5.py

Paliz Portal - Cross-Site Scripting / Multiple SQL Injections
| asp/webapps/359[01;31m[K23[m[K.txt
```

Panda ActiveScan 5.0 - 'ascontrol.dll' Denial of Service
| windows/dos/[01;31m[K23[m[K918.txt

Panda ActiveScan 5.0 - 'ascontrol.dll' Remote Heap Overflow
| windows/dos/[01;31m[K23[m[K917.txt

Panda Global Protection 2010 - Local Denial of Service (unfiltered wcscpy()) |
windows/dos/160[01;31m[K23[m[K.c

Pango Font Parsing - 'pangoft2-render.c' Heap Corruption
| linux/remote/35[01;31m[K23[m[K2.txt

Parallels H-Sphere 3.0/3.1 - 'login.php' Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/3[01;31m[K23[m[K96.txt

Paranews 3.4 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K23[m[K65.txt

Parnian Opendata CMS - SQL Injection
| php/webapps/17[01;31m[K23[m[K1.txt

Parrot and DJI variants Drone OSes - Kernel Panic Exploit
| multiple/local/5[01;31m[K23[m[K29.py

ParsBlogger - 'blog.asp' SQL Injection
| php/webapps/7[01;31m[K23[m[K9.txt

PaulShop - SQL Injection / Cross-Site Scripting
| php/webapps/4[01;31m[K23[m[K59.txt

Pay Banner Text Link Ad 1.0.6.1 - SQL Injection
| php/webapps/426[01;31m[K23[m[K.txt

PayPal Store Front 3.0 - 'index.php' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K[01;31m[K23[m[K2.txt

PayProCart 1146078425 - Multiple Remote File Inclusions
| php/webapps/[01;31m[K23[m[K16.txt

PBLang 4.65 Bulletin Board System - 'SetCookie.php' Directory Traversal
| php/webapps/26[01;31m[K23[m[K1.txt

PC Tools Firewall Plus 7.0.0.1[01;31m[K23[m[K - Local Denial of Service
| windows/dos/19453.cpp

PCMan FTP Server 2.0.7 - Buffer Overflow
| windows/remote/5[01;31m[K23[m[K26.txt

PEGA Platform <= 7.2 ML0 - Missing Access Control / Cross-Site Scripting |
multiple/webapps/4[01;31m[K23[m[K35.txt

Pegasi Web Server 0.2.2 - Arbitrary File Access
| linux/remote/[01;31m[K23[m[K802.txt

Pegasi Web Server 0.2.2 - Error Page Cross-Site Scripting
| linux/remote/[01;31m[K23[m[K803.txt

Pelco Sarix/Spectra Cameras - Cross-Site Request Forgery (Enable SSH Root Access) |
hardware/webapps/4[01;31m[K23[m[K08.txt

Pelco Sarix/Spectra Cameras - Cross-Site Request Forgery / Cross-Site Scripting |
hardware/webapps/4[01;31m[K23[m[K07.txt

Pelco Sarix/Spectra Cameras - Remote Code Execution
| hardware/webapps/4[01;31m[K23[m[K09.txt

Pelco VideoXpert 1.12.105 - Directory Traversal
| windows/webapps/4[01;31m[K23[m[K11.txt

Pelco VideoXpert 1.12.105 - Information Disclosure
| windows/webapps/4[01;31m[K23[m[K12.txt

Pelco VideoXpert 1.12.105 - Local Privilege Escalation
| windows/local/4[01;31m[K23[m[K10.txt

Perforce P4Web - Multiple Cross-Site Scripting Vulnerabilities
| jsp/webapps/38[01;31m[K23[m[K5.txt

pfSense 2.0.1 - Cross-Site Scripting / Cross-Site Request Forgery / Remote Command Execution |
php/webapps/[01;31m[K23[m[K901.txt

PG Dating Pro CMS 1.0 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K23[m[K73.txt

PGN2WEB 0.3 - Remote Buffer Overflow
| windows/remote/250[01;31m[K23[m[K.txt

PGP4Pine 1.75.6/1.76 - 'Message Line' Remote Buffer Overflow
| linux/remote/2[01;31m[K23[m[K46.c

PHlyMail Lite 3.4.4 - 'folderprops.php' Remote File Inclusion (2)
| php/webapps/2[01;31m[K23[m[K6.txt

Phorum 3.x - 'login.php' HTTP_REFERER Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K819.txt

Phorum 3.x - 'profile.php?target' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K820.txt

Phorum 3.x - 'register.php' HTTP_REFERER Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K818.txt

```
Phorum 5.0.14 - Multiple Subject and Attachment HTML Injection
Vulnerabilities                                 |
php/webapps/252[01;31m[K23[m[K.txt

Phorum 5.2.11 - Persistent Cross-Site Scripting
| php/webapps/9[01;31m[K23[m[K1.txt

PhotoKorn Gallery 1.52 - 'dir_path' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K27.txt

PhotoPost 4.6 - 'PP_PATH' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K69.txt

PhotoPost PHP Pro 3.x/4.x - 'showgallery.php' Multiple SQL Injections
| php/webapps/[01;31m[K23[m[K885.txt

PhotoShow 3.0 - Remote Code Execution
| php/webapps/51[01;31m[K23[m[K6.py

PHP 4.x - DLOpen Memory Disclosure (1)
| php/local/[01;31m[K23[m[K022.c

PHP 4.x - DLOpen Memory Disclosure (2)
| php/local/[01;31m[K23[m[K0[01;31m[K23[m[K.c

PHP 5.2 - Session.Save_Path() 'Safe_mode' / 'open_basedir' Restriction
Bypass                                | php/local/29[01;31m[K23[m[K9.txt

PHP 5.2.1 'GD' Extension - '.WBMP' File Integer Overflow
| php/dos/298[01;31m[K23[m[K.c

PHP 5.2.5 - Multiple functions 'safe_mode_exec_dir' / 'open_basedir'
Restriction Bypass Vulnerabilities    |
php/local/3[01;31m[K23[m[K43.php

PHP 5.4.3 - apache_request_headers Function Buffer Overflow
(Metasploit)                                      |
windows/remote/19[01;31m[K23[m[K1.rb

PHP 5.5.37/5.6.[01;31m[K23[m[K/7.0.8 - 'bzread()' Out-of-Bounds Write
| php/dos/40155.py

PHP 5.x - 'Win32service' Local 'Safe_Mode()' Bypass
| windows/local/4[01;31m[K23[m[K6.php

PHP Car Rental-Script - Authentication Bypass
| php/webapps/113[01;31m[K23[m[K.txt

PHP CGI Module 8.3.4 - Remote Code Execution (RCE)
| php/webapps/5[01;31m[K23[m[K31.py

PHP Chat for 1[01;31m[K23[m[K Flash Chat - Remote File Inclusion
| php/webapps/14425.txt
```

PHP Classifieds 6.09 - E-mail Dump
| php/webapps/1[01;31m[K23[m[K86.txt

PHP Classifieds Rental Script 3.6.0 - 'scatid' SQL Injection
| php/webapps/415[01;31m[K23[m[K.txt

PHP DocWriter 0.3 - 'script' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K73.py

PHP Melody 1.5.3 - Arbitrary File Upload Injection
| php/webapps/9[01;31m[K23[m[K9.txt

PHP MicroCMS 1.0.1 - Cross-Site Request Forgery / Cross-Site Scripting
| php/webapps/159[01;31m[K23[m[K.txt

PHP Pro Bid 5.2.4/6.04 - Multiple SQL Injections
| php/webapps/3[01;31m[K23[m[K97.txt

PHP Session Deserializer - Use-After-Free
| php/dos/381[01;31m[K23[m[K.txt

PHP Website 0.7.3/0.8.2/0.8.3/0.9.2 Calendar Module - SQL Injection
| php/webapps/[01;31m[K23[m[K013.txt

PHP-Address Book 4.0.x - Multiple SQL Injections
| php/webapps/90[01;31m[K23[m[K.txt

PHP-Coolfile 1.4 - Unauthorized Administrative Access
| php/webapps/[01;31m[K23[m[K372.txt

PHP-Fusion 6.00.109 - 'msg_send' SQL Injection
| php/webapps/1[01;31m[K23[m[K7.php

PHP-Nuke 1.0/2.5/3.0/4.x/5.x/6.x/7.x - Multiple Vulnerabilities
| php/webapps/24[01;31m[K23[m[K2.txt

PHP-Nuke 4.x/5.x - Arbitrary File Inclusion
| php/webapps/21[01;31m[K23[m[K0.txt

PHP-Nuke 4.x/5.x - SQL_Debug Information Disclosure
| php/webapps/21[01;31m[K23[m[K3.txt

PHP-Nuke 5.5/6.0 AvantGo Module - Full Path Disclosure
| php/webapps/2[01;31m[K23[m[K47.txt

PHP-Nuke 5.5/6.0 News Module - Full Path Disclosure
| php/webapps/2[01;31m[K23[m[K48.txt

PHP-Nuke 6.0/6.5 Forum Module - 'viewtopic.php' SQL Injection
| php/webapps/224[01;31m[K23[m[K.txt

PHP-Nuke 6.6 - 'admin.php' SQL Injection
| php/webapps/[01;31m[K23[m[K[01;31m[K23[m[K7.pl

```
PHP-Nuke 6.x (Multiple Modules) - SQL Injection
| php/webapps/[01;31m[K23[m[K631.txt

PHP-Nuke 6.x - 'Category' SQL Injection
| php/webapps/[01;31m[K23[m[K680.php

PHP-Nuke 6.x/7.0 'News' Module - Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K663.txt

PHP-Nuke 6.x/7.0 Survey Module - SQL Injection
| php/webapps/[01;31m[K23[m[K484.txt

PHP-Nuke 6.x/7.0/7.1 - Image Tag Admin Command Execution
| php/webapps/[01;31m[K23[m[K835.txt

PHP-Nuke 6.x/7.x 'Reviews' Module - Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K669.txt

PHP-Nuke 6.x/7.x - CookieDecode Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K990.txt

PHP-Nuke 6.x/7.x - Multiple SQL Injections
| php/webapps/[01;31m[K23[m[K998.txt

PHP-Nuke 6.x/7.x - Public Message SQL Injection
| php/webapps/[01;31m[K23[m[K670.pl

PHP-Nuke 7.1 Recommend_Us Module - 'fname' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K814.txt

PHP-Nuke 7.5 < 7.8 - 'Search' SQL Injection
| php/webapps/15[01;31m[K23[m[K.cpp

PHP-Nuke 8.2.4 - Cross-Site Request Forgery
| php/webapps/[01;31m[K23[m[K289.txt

PHP-Nuke Error Manager Module 2.1 - 'error.php' Multiple Cross-Site
Scripting Vulnerabilities              |
php/webapps/[01;31m[K23[m[K845.txt

PHP-Nuke Error Manager Module 2.1 - 'error.php?language' Full Path
Disclosure                              |
php/webapps/[01;31m[K23[m[K844.txt

PHP-Nuke Module PostGuestbook 0.6.1 - 'tpl_pgb_moddir' Remote File
Inclusion                               |
php/webapps/34[01;31m[K23[m[K.txt

PHP-Nuke MS-Analysis Module - HTTP Referrer Field SQL Injection
| php/webapps/[01;31m[K23[m[K870.txt
```

PHP-Nuke MS-Analysis Module - Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/[01;31m[K23[m[K869.txt

PHP-Nuke Splatt Forum 3.2 Module - Full Path Disclosure
| php/webapps/2[01;31m[K23[m[K49.txt

PHP-ping - 'Count' Command Execution
| php/webapps/[01;31m[K23[m[K487.txt

PHP1[01;31m[K23[m[K Top Sites - 'category.php?cat' SQL Injection
| php/webapps/4241.txt

phpAdultSite CMS - 'results_per_page' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K38.txt

phpBazar-2.1.1fix - Remote Administration-Panel
| php/webapps/10[01;31m[K23[m[K3.txt

phpBB 1.x/2.0.x - 'search.php?search_results' SQL Injection
| php/webapps/[01;31m[K23[m[K821.php

phpBB 1.x/2.0.x - Multiple Input Validation Vulnerabilities
| php/webapps/[01;31m[K23[m[K866.txt

phpBB 2.0.21 - Poison Null Byte Remote File Upload
| php/webapps/[01;31m[K23[m[K48.pl

phpBB 2.0.6 - 'privmsg.php' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K475.txt

phpBB 2.0.6 - URL BBCode HTML Injection
| php/webapps/[01;31m[K23[m[K125.txt

phpBB 2.0.x - 'profile.php' Cross-Site Scripting
| php/webapps/255[01;31m[K23[m[K.txt

phpBB 2.0.x - 'profile.php' SQL Injection
| php/webapps/[01;31m[K23[m[K363.txt

phpBB Minerva Mod 2.0.21 build [01;31m[K23[m[K8a - SQL Injection
| php/webapps/3519.txt

phpBB Mod FileBase 2.0 - 'id' SQL Injection
| php/webapps/5[01;31m[K23[m[K6.txt

phpBB Shadow Premod 2.7.1 - Remote File Inclusion
| php/webapps/[01;31m[K23[m[K11.txt

phpBB Tweaked 3 - 'phpbb_root_path' Remote File Inclusion
| php/webapps/3[01;31m[K23[m[K5.txt

```
phpBB XS 0.58 - 'functions.php' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K49.txt

PHPBB2 MODificat 0.2.0 - 'functions.php' Remote File Inclusion
| php/webapps/3[01;31m[K23[m[K1.txt

Phpclanwebsite 1.[01;31m[K23[m[K.1 - BBCode IMG Tag Script Injection
| php/webapps/27109.txt

Phpclanwebsite 1.[01;31m[K23[m[K.1 - SQL Injection
| php/webapps/1453.pl

phpclanwebsite 1.[01;31m[K23[m[K.3 fix pack #5 - Multiple
Vulnerabilities                                                 |
php/webapps/7515.txt

phpCMS 2008 V2 - 'data.php' SQL Injection
| php/webapps/35[01;31m[K23[m[K9.txt

PhpCommander 3.0 - 'upload' Remote Code Execution
| php/webapps/[01;31m[K23[m[K10.php

phpCommunityCalendar 4.0 - Multiple Cross-Site Scripting
Vulnerabilities                                 |
php/webapps/26[01;31m[K23[m[K2.txt

phpegasus 0.1.2 - 'FCKeditor' Arbitrary File Upload
| php/webapps/1[01;31m[K23[m[K81.php

phpFullAnnu 5.1 - 'repmod' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K13.txt

PHPGedView 2.61 - Multiple Remote File Inclusions
| php/webapps/[01;31m[K23[m[K520.txt

PhpGedView 2.61 - PHPInfo Information Disclosure
| php/webapps/[01;31m[K23[m[K526.txt

PhpGedView 2.61 - Search Script Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K525.txt

PHPGedView 2.x - 'Editconfig_gedcom.php' Directory Traversal
| php/webapps/[01;31m[K23[m[K616.txt

PHPGedView 2.x - '[GED_File]_conf.php' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K617.txt

phpGreetCards 3.7 - Cross-Site Scripting
| php/webapps/1[01;31m[K23[m[K45.txt

PHPix 2.0.3 - Arbitrary Command Execution
| php/webapps/[01;31m[K23[m[K558.txt
```

PHPKit 1.6 - 'Include.php' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K333.txt

phpLDAPadmin 0.9.4b - Denial of Service
| php/dos/180[01;31m[K23[m[K.java

PhpLinkExchange 1.0 - Include / Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K47.txt

phpMyAdmin 2.x - 'Export.php' File Disclosure
| php/webapps/[01;31m[K23[m[K640.txt

phpMyAdmin 3.2 - 'server_databases.php' Remote Command Execution
| php/webapps/3[01;31m[K23[m[K83.txt

phpMyFAQ 3.2.10 - Unintended File Download Triggered by Embedded Frames
| php/webapps/52[01;31m[K23[m[K5.txt

phpMyNewsletter 0.8b5 - 'msg_id' SQL Injection
| php/webapps/5[01;31m[K23[m[K1.php

PHPMyRing 4.1.3b - 'fichier' Remote File Inclusion
| php/webapps/3[01;31m[K23[m[K8.txt

PhpNews 1.0 - 'Include' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K[01;31m[K23[m[K.txt

phpNewsManager 1.36 - functions Script File Disclosure
| php/webapps/[01;31m[K23[m[K742.txt

PHPOpenChat 3.0.1 - Multiple HTML Injection Vulnerabilities
| php/webapps/25[01;31m[K23[m[K6.html

PHPOutsourcing Zorum 3.4 - Full Path Disclosure
| php/webapps/[01;31m[K23[m[K018.txt

PHPOutSourcing Zorum 3.x - Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K011.txt

PHPPing 0.1 - Remote Command Execution
| php/webapps/2[01;31m[K23[m[K36.txt

phpQuiz 0.1 - 'pagename' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K66.txt

phpQuiz 0.1.2 - SQL Injection / Code Execution
| php/webapps/[01;31m[K23[m[K76.pl

PHProjekt 6.1 - 'path_pre' Multiple Remote File Inclusions
| php/webapps/2[01;31m[K23[m[K5.txt

```
phpShop Web Shopping Cart 0.6.1 -b - Multiple Function Cross-Site
Scripting Vulnerabilities                |
php/webapps/[01;31m[K23[m[K546.txt

phpSQLiteCMS 1 RC2 - '/cms/includes/header.inc.php' Multiple Cross-Site
Scripting Vulnerabilities          | php/webapps/318[01;31m[K23[m[K.txt

phpunity.postcard - 'gallery_path' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K57.txt

PHPWCMS 1.5.4.6 - 'preg_replace' Multiple Vulnerabilities
| php/webapps/[01;31m[K23[m[K448.php

PHPWebFileManager 2.0 - 'index.php' Directory Traversal
| php/webapps/[01;31m[K23[m[K381.txt

phpWebSite 0.7.3/0.8.2/0.8.3/0.9.2 Calendar Module - 'day' Cross-Site
Scripting                              |
php/webapps/[01;31m[K23[m[K014.txt

phpWebSite 0.7.3/0.8.2/0.8.3/0.9.2 earch Module - 'PDA_limit' Cross-
Site Scripting                          |
php/webapps/[01;31m[K23[m[K017.txt

phpWebSite 0.7.3/0.8.2/0.8.3/0.9.2 fatcat Module - 'fatcat_id' Cross-
Site Scripting                          |
php/webapps/[01;31m[K23[m[K015.txt

phpWebSite 0.7.3/0.8.2/0.8.3/0.9.2 pagemaster Module - 'PAGE_id' Cross-
Site Scripting                         |
php/webapps/[01;31m[K23[m[K016.txt

PHPWeby Free Directory Script - 'contact.php' Multiple SQL Injections
| php/webapps/38[01;31m[K23[m[K8.txt

PHPX 3.2.3 - Multiple Vulnerabilities
| php/webapps/[01;31m[K23[m[K644.php

PhreeBooks ERP 5.2.5 - Remote Command Execution
| php/webapps/484[01;31m[K23[m[K.txt

PicoPhone Internet Phone 1.63 - Remote Buffer Overflow
| hardware/dos/[01;31m[K23[m[K876.txt

Pie Cart Pro - 'Home_Path' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K92.txt

Pie Cart Pro - 'Inc_Dir' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K93.txt

Pimcore CMS 2.3.0/3.0 - SQL Injection
| multiple/webapps/356[01;31m[K23[m[K.txt
```

```
Pine (Local Message Grabber) - Local Message Read
| linux/local/[01;31m[K23[m[K1.sh

PInfo 0.6.9-5.1 - Local Buffer Overflow
| linux/local/400[01;31m[K23[m[K.py

Pinger 1.0 - Remote Code Execution
| php/webapps/483[01;31m[K23[m[K.txt

Pivot 1.40.6 - Arbitrary File Deletion
| php/webapps/8[01;31m[K23[m[K9.txt

PixelPost 1.4.3 - User Comment HTML Injection
| php/webapps/271[01;31m[K23[m[K.txt

Pixie 1.04 - Blog Post Cross-Site Request Forgery
| php/webapps/18[01;31m[K23[m[K6.txt

PJ CGI Neo Review - Directory Traversal
| cgi/webapps/[01;31m[K23[m[K615.txt

Plane 0.[01;31m[K23[m[K.1 - Server side request forgery (SSRF)
| multiple/webapps/52211.txt

Platform Load Sharing Facility 4/5/6 - 'EAuth' Local Privilege
Escalation                                    |
linux/local/[01;31m[K23[m[K743.txt

PLD Software Ebola 0.1.4 - Remote Buffer Overflow
| linux/remote/[01;31m[K23[m[K413.c

Plex Media Server 0.9.9.2.374-aa[01;31m[K23[m[Ka69 - Multiple
Vulnerabilities                                          |
multiple/webapps/31983.txt

Plug and Play Web Server 1.0 002c - Directory Traversal
| windows/remote/[01;31m[K23[m[K157.txt

Plug And Play Web Server 1.0 002c - FTP Service Command Handler Buffer
Overflow                           | windows/dos/[01;31m[K23[m[K166.pl

PNPHPBB2 < 1.2g - 'phpbb_root_path' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K90.txt

Polycom Shell HDX Series - Traceroute Command Execution (Metasploit)
| unix/remote/43[01;31m[K23[m[K0.rb

Popper 1.41-r2 - 'form' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K51.txt

Post Affiliate Pro 3 - 'umprof_status' Blind SQL Injection
| php/webapps/7[01;31m[K23[m[K8.txt
```

```
Poster 2.0 - Unauthorized Privileged User Access
| asp/webapps/[01;31m[K23[m[K035.txt

PostMaster 3.16/3.17 Proxy Service - Cross-Site Scripting
| multiple/remote/[01;31m[K23[m[K385.txt

PostNuke 0.7[01;31m[K23[m[K - 'user.php' UNAME Cross-Site Scripting
| php/webapps/22767.txt

PostNuke 0.7[01;31m[K23[m[K - Multiple Cross-Site Scripting
Vulnerabilities                                              |
php/webapps/22761.txt

Power Audio Editor 7.4.3.[01;31m[K23[m[K0 - '.cda' Denial of Service
| windows/dos/15495.py

Powered by iNetScripts - Arbitrary File Upload
| php/webapps/1[01;31m[K23[m[K84.txt

PowerMovieList 0.13/0.14 - Edit User HTML Injection
| php/webapps/288[01;31m[K23[m[K.pl

pPIM 1.0 - Upload/Change Password
| php/webapps/6[01;31m[K23[m[K1.txt

Print Job Accounting 4.4.10 - 'OkiJaSvc' Unquoted Service Path
| windows/local/496[01;31m[K23[m[K.txt

Privacy Drive v3.17.0 - 'pdsvc.exe' Unquoted Service Path
| windows/local/490[01;31m[K23[m[K.txt

Private Message System 2.x - 'index.php?Page' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K486.txt

ProConf 6.0 -  Insecure Direct Object Reference (IDOR)
| multiple/webapps/52[01;31m[K23[m[K6.txt

ProductCart 1.x/2.x - 'advSearch_h.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K23[m[K703.txt

ProductCart 1.x/2.x - 'Custva.asp?redirectUrl' Cross-Site Scripting
| asp/webapps/[01;31m[K23[m[K704.txt

ProductCart 1.x/2.x - Weak Cryptography
| asp/webapps/[01;31m[K23[m[K702.txt

ProficySCADA for iOS 5.0.25920 - 'Password' Denial of Service (PoC)
| ios/dos/48[01;31m[K23[m[K6.py

ProFTPd 1.2.7/1.2.8 - '.ASCII' File Transfer Buffer Overrun
| linux/dos/[01;31m[K23[m[K170.c
```

```
Progress OpenEdge 10b - Multiple Denial of Service Vulnerabilities
| windows/dos/300[01;31m[K23[m[K.txt

Project Based Calendaring System (PBCS) 0.7.1 - Multiple
Vulnerabilities                                      |
php/webapps/55[01;31m[K23[m[K.txt

Project64 2.3.2 - Buffer Overflow (SEH)
| windows_x86/local/45[01;31m[K23[m[K5.py

ProjectForum 8.4.2.1 - Find Request Denial of Service
| php/dos/[01;31m[K23[m[K460.pl

projectSend r1605 - Remote Code Exectution RCE
| php/webapps/51[01;31m[K23[m[K8.txt

PROMOTIC 8.1.3 - Multiple Vulnerabilities
| windows/remote/36[01;31m[K23[m[K5.txt

ProSSHD 1.2 20090726 - Denial of Service (DoS)
| windows/remote/5[01;31m[K23[m[K21.NA

Prototype of an PHP Application 0.1 - '/ident/index.php?path_inc'
Remote File Inclusion                    |
php/webapps/301[01;31m[K23[m[K.txt

Proxy-Pro Professional GateKeeper 4.7 Web Proxy - Buffer Overrun
| windows/remote/[01;31m[K23[m[K741.c

Prozilla 1.3.7.4 - 'ftpsearch' Results Handling Buffer Overflow
| linux/remote/1[01;31m[K23[m[K8.c

PSCS VPOP3 2.0 Email Server WebAdmin - Cross-Site Scripting
| multiple/remote/[01;31m[K23[m[K271.txt

PSOProxy 0.91 - Remote Buffer Overflow (1)
| windows/remote/[01;31m[K23[m[K732.c

PSOProxy 0.91 - Remote Buffer Overflow (2)
| windows/remote/[01;31m[K23[m[K733.c

PSOProxy 0.91 - Remote Buffer Overflow (3)
| windows/remote/[01;31m[K23[m[K734.c

Psychoblogger PB-beta1 - 'desc' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K477.txt

Psychoblogger PB-beta1 - errormessage Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K478.txt

PUMA 1.0 RC 2 - 'config.php' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K40.txt
```

PunBB 1.2.3 - Multiple HTML Injection Vulnerabilities
| php/webapps/25[01;31m[K23[m[K0.txt

PWebServer 0.3.x - Directory Traversal
| linux/remote/[01;31m[K23[m[K794.txt

PXE Server 2.0 - Remote Buffer Overrun
| linux/remote/2[01;31m[K23[m[K79.c

PY Software Active Webcam 4.3 - WebServer Cross-Site Scripting
| windows/remote/[01;31m[K23[m[K451.txt

PY Software Active Webcam 4.3 - WebServer Directory Traversal
| windows/remote/[01;31m[K23[m[K450.txt

Py-Membres 4.x - 'Pass_done.php' SQL Injection
| php/webapps/[01;31m[K23[m[K061.txt

Py-Membres 4.x - 'Secure.php' Unauthorized Access
| php/webapps/[01;31m[K23[m[K060.txt

Python 1.5.2 Pickle - Unsafe 'eval()' Code Execution
| linux/local/216[01;31m[K23[m[K.txt

python-wrapper - Untrusted Search Path/Code Execution
| linux/local/195[01;31m[K23[m[K.txt

Q-Shop 3.5 - 'browse.asp' SQL Injection
| asp/webapps/[01;31m[K23[m[K84.txt

QNAP QVR Client 5.0.0.13[01;31m[K23[m[K0 - 'QVRService' Unquoted
Service Path |
windows/local/49645.txt

QNap QVR Client 5.0.3.[01;31m[K23[m[K100 - Denial of Service (PoC)
| windows_x86-64/dos/45162.py

QNX 6.4.0 - bitflipped ELF Binary 'id' Kernel Panic (Denial of Service)
| qnx/dos/78[01;31m[K23[m[K.txt

Qpopper 3/4 - 'Username' Information Disclosure
| linux/remote/2[01;31m[K23[m[K61.cpp

Qpopper 4.0.8 (FreeBSD) - Local Privilege Escalation
| bsd/local/1[01;31m[K23[m[K0.sh

Qpopper 4.0.x - Remote Memory Corruption
| linux/remote/2[01;31m[K23[m[K42.c

QtWeb 3.0 - Remote Crash (Denial of Service)
| windows/dos/11[01;31m[K23[m[K3.pl

Qualcomm Eudora 5.0/5.1/6.0 - Long Attachment Filename Denial of Service (1) | windows/dos/2[01;31m[K23[m[K33.pl

Qualcomm Eudora 5.0/5.1/6.0 - Long Attachment Filename Denial of Service (2) | windows/dos/2[01;31m[K23[m[K34.pl

Qualcomm Eudora 5.x/6.0 - Spoofed Attachment Line Denial of Service | windows/dos/[01;31m[K23[m[K374.pl

Qualcomm Eudora 6.0.1/6.1.1 - Attachment LaunchProtect Warning Bypass (1) | windows/remote/[01;31m[K23[m[K398.pl

Qualcomm Eudora 6.0.1/6.1.1 - Attachment LaunchProtect Warning Bypass (2) | windows/remote/[01;31m[K23[m[K399.pl

Qualiteam X-Cart 3.x - 'general.php?perl_binary' Arbitrary Command Execution | php/webapps/[01;31m[K23[m[K636.txt

Qualiteam X-Cart 3.x - 'upgrade.php?perl_binary' Arbitrary Command Execution | php/webapps/[01;31m[K23[m[K637.txt

Qualiteam X-Cart 3.x - Multiple Remote Information Disclosure Vulnerabilities | php/webapps/[01;31m[K23[m[K639.txt

Quantum DXi V1000 2.2.1 - Static SSH Key | unix/remote/3[01;31m[K23[m[K72.txt

Quantum vmPRO - Backdoor Command (Metasploit) | unix/remote/3[01;31m[K23[m[K67.rb

Quantum vmPRO 3.1.2 - Local Privilege Escalation | hardware/local/3[01;31m[K23[m[K70.txt

Quick Cart 3.1 - 'admin.php' Cross-Site Scripting | php/webapps/3[01;31m[K23[m[K89.txt

Quick CMS Lite 2.1 - 'admin.php' Cross-Site Scripting | php/webapps/3[01;31m[K23[m[K87.txt

Quicksilver Forums 1.2.1 - Remote File Inclusion | php/webapps/[01;31m[K23[m[K56.txt

Quicksilver Forums 1.4.1 - SQL Injection | php/webapps/62[01;31m[K23[m[K.php

```
QuicO - 'photo.php' SQL Injection
| php/webapps/3[01;31m[K23[m[K66.txt

Qvod Player 2.1.5 - 'QvodInsert.dll' ActiveX Control Remote Buffer
Overflow                                  |
windows/remote/310[01;31m[K23[m[K.html

Radio istek scripti 2.5 - Remote Configuration Disclosure
| php/webapps/10[01;31m[K23[m[K1.txt

RaidenHTTPD 1.1.49 - 'SoftParserFileXml' Remote Code Execution
| windows/remote/[01;31m[K23[m[K28.php

RARLAB WinRAR 3.x - LHA Filename Handling Buffer Overflow
| windows/remote/28[01;31m[K23[m[K5.c

Razer Synapse 2.20.15.1104 - rzpnk.sys ZwOpenProcess (Metasploit)
| windows_x86-64/local/4[01;31m[K23[m[K68.rb

Rconfig 3.x - Chained Remote Code Execution (Metasploit)
| linux/remote/482[01;31m[K23[m[K.rb

Realestate Crowdfunding Script 2.7.2 - 'pid' SQL Injection
| php/webapps/43[01;31m[K23[m[K9.txt

Really Simple PHP and Ajax (RSPA) 2007-03-[01;31m[K23[m[K - Remote File
Inclusion                                        | php/webapps/3641.txt

RealNetworks RealPlayer - Denial of Service
| multiple/dos/386[01;31m[K23[m[K.html

RealOne Player 1.0/2.0/6.0.10/6.0.11 - '.SMIL' File Script Execution
| windows/remote/[01;31m[K23[m[K043.txt

RealOne Player for Linux 2.2 Alpha - Insecure Configuration File
Permission Privilege Escalation           |
linux/local/[01;31m[K23[m[K126.c

RealPlayer - '.RealMedia' File Handling Buffer Overflow (Metasploit)
| windows/remote/[01;31m[K23[m[K694.rb

RealPlayer/Helix Player (Linux) - Remote Format String
| linux/remote/1[01;31m[K23[m[K2.c

RealServer < 8.0.2 (Windows Platforms) - Remote Overflow
| windows/remote/[01;31m[K23[m[K.c

ReCMS - 'users_lang' Directory Traversal
| php/webapps/34[01;31m[K23[m[K6.txt

Red-M Red-Alert 3.1 - Remote Denial of Service
| hardware/dos/[01;31m[K23[m[K672.txt
```

RedaxScript CMS 2.2.0 - SQL Injection
| php/webapps/360[01;31m[K23[m[K.txt

RedBlog 0.5 - 'index.php' Remote File Inclusion
| php/webapps/284[01;31m[K23[m[K.txt

REDDOXX Appliance Build 2032 / 2.0.625 - Arbitrary File Disclosure
| json/webapps/4[01;31m[K23[m[K72.txt

REDDOXX Appliance Build 2032 / 2.0.625 - Remote Command Execution
| json/webapps/4[01;31m[K23[m[K71.txt

RedHat 6.1/6.2 - TTY Flood Users
| linux/dos/[01;31m[K23[m[K6.sh

RedHat 8/9 - Directory Server Crafted Search Pattern Denial of Service
| linux/dos/3[01;31m[K23[m[K04.txt

RedHat Apache 2.0.40 - Directory Index Default Configuration Error
| linux/remote/[01;31m[K23[m[K296.txt

RedStorm Ghost Recon Game Engine - Remote Denial of Service
| multiple/dos/[01;31m[K23[m[K755.txt

reget deluxe 3.0 build 121 - Directory Traversal
| jsp/webapps/[01;31m[K23[m[K872.txt

Relative Real Estate Systems 1.2 - SQL Injection
| php/webapps/267[01;31m[K23[m[K.txt

RemotelyAnywhere - Default.HTML Logout Message Injection
| cgi/webapps/[01;31m[K23[m[K432.txt

Reptile Web Server Reptile Web Server 20020105 - Denial of Service
| multiple/dos/[01;31m[K23[m[K590.txt

Request It 1.0b - 'index.php?id' Remote File Inclusion
| php/webapps/37[01;31m[K23[m[K.txt

Restorator 1793 - Denial of Service (PoC)
| windows_x86-64/dos/452[01;31m[K23[m[K.py

ReVou Twitter Clone - Admin Password Change
| php/webapps/75[01;31m[K23[m[K.php

REZERVI 3.0.2 - Remote Command Execution
| php/webapps/125[01;31m[K23[m[K.py

RhinoSoft Serv-U FTPd Server 3/4 - MDTM Command Stack Overflow (1)
| windows/remote/[01;31m[K23[m[K591.c

RhinoSoft Serv-U FTPd Server 3/4 - MDTM Command Stack Overflow (2)
| windows/remote/[01;31m[K23[m[K592.c

RhinoSoft Serv-U FTPd Server 3/4/5 - 'MDTM' Time Argument Buffer Overflow (1) | windows/dos/[01;31m[K23[m[K760.pl

RhinoSoft Serv-U FTPd Server 3/4/5 - 'MDTM' Time Argument Buffer Overflow (2) | windows/dos/[01;31m[K23[m[K761.c

RhinoSoft Serv-U FTPd Server 3/4/5 - 'MDTM' Time Argument Buffer Overflow (3) | windows/dos/[01;31m[K23[m[K762.c

RhinoSoft Serv-U FTPd Server 3/4/5 - MDTM Command Time Argument Buffer Overflow (4) | windows/remote/[01;31m[K23[m[K763.c

Rlpr 2.0 - 'msg()' Multiple Vulnerabilities
| linux/remote/242[01;31m[K23[m[K.py

RM Downloader 2.50.60 2006.06.[01;31m[K23[m[K - 'Load' Local Buffer Overflow (EggHunter) (SEH) (PoC) | windows/local/48628.py

RM Downloader 3.0.2.1 - '.m3u' Local Stack Overflow
| windows/local/104[01;31m[K23[m[K.pl

RobotFTP Server 1.0/2.0 - 'Username' Buffer Overflow (1)
| windows/dos/[01;31m[K23[m[K708.c

RobotFTP Server 1.0/2.0 - 'Username' Buffer Overflow (2)
| windows/dos/[01;31m[K23[m[K709.c

RobotFTP Server 1.0/2.0 - Remote Denial of Service
| php/dos/[01;31m[K23[m[K750.txt

Roger Wilco 1.4.1 - Remote Server Side Buffer Overrun
| windows/remote/[01;31m[K23[m[K1[01;31m[K23[m[K.pl

Roger Wilco Server 1.4.1 - UDP Datagram Handling Denial of Service
| multiple/dos/[01;31m[K23[m[K902.txt

Roger Wilco Server 1.4.1 - Unauthorized Audio Stream Denial of Service
| multiple/dos/[01;31m[K23[m[K904.txt

Roundcube 1.6.10 - Remote Code Execution (RCE)
| multiple/webapps/5[01;31m[K23[m[K24.NA

RSA ClearTrust 4.6/4.7 - Login Page Cross-Site Scripting
| asp/webapps/2[01;31m[K23[m[K57.txt

Ruby 1.9 - regex engine Remote Socket Memory Leak
| multiple/dos/6[01;31m[K23[m[K9.txt

```
Ruby 1.9 dl - Module DL.dlopen Arbitrary Library Access
| multiple/remote/322[01;31m[K23[m[K.rb

Rukovoditel 2.6.1 - RCE (1)
| php/webapps/49[01;31m[K23[m[K8.sh

Rumba FTP Client 4.2 - PASV Buffer Overflow (SEH)
| windows/remote/1[01;31m[K23[m[K80.pl

Rumble 0.25.2[01;31m[K23[m[K2 - Denial of Service
| windows/dos/17070.py

RunCMS 1.1 - Database Configuration Information Disclosure
| php/webapps/25[01;31m[K23[m[K7.txt

RXGoogle.CGI 1.0/2.5 - Cross-Site Scripting
| cgi/webapps/[01;31m[K23[m[K647.txt

S9Y Serendipity Freetag-plugin 3.[01;31m[K23[m[K -
'serendipity[tagview]' Cross-Site Scripting                          |
php/webapps/36168.txt

Salim Gasmi GLD (Greylisting Daemon) 1.0 < 1.4 - Postfix Greylisting
Buffer Overflow (Metasploit)          |
linux/remote/100[01;31m[K23[m[K.rb

Sama Educational Management System - 'error.asp' Cross-Site Scripting
| asp/webapps/3[01;31m[K23[m[K94.txt

SamaGraph CMS - 'inside.aspx' SQL Injection
| asp/webapps/339[01;31m[K23[m[K.txt

Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege
Escalation                            |
linux/local/[01;31m[K23[m[K674.txt

Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Overflow
| unix/remote/2[01;31m[K23[m[K56.c

Sambar Server 4.3/4.4 Beta 3 - Search CGI
| windows/remote/202[01;31m[K23[m[K.txt

Sambar Server 6.0 - 'results.stm' POST Buffer Overflow
| windows/dos/[01;31m[K23[m[K664.py

Samhain Labs 1.x - HSFTP Remote Format String
| linux/remote/[01;31m[K23[m[K740.c

Sami FTP Server 1.1.3 - Invalid Command Argument Local Denial of
Service                                 |
windows/dos/[01;31m[K23[m[K692.txt
```

Sami FTP Server 1.1.3 - Library Crafted GET Remote Denial of Service
| windows/dos/[01;31m[K23[m[K693.txt

Sami FTP Server 2.0.1 - MKD Buffer Overflow ASLR Bypass (SEH)
| windows/remote/275[01;31m[K23[m[K.py

Samsung Smart Home Camera SNH-P-6410 - Command Injection
| hardware/remote/40[01;31m[K23[m[K5.py

SAP Business Connector 4.6/4.7 - 'adapter-index.dsp?url' Arbitrary Site Redirect |
linux/remote/27[01;31m[K23[m[K5.txt

SAP Business Connector 4.6/4.7 - 'chopSAPLog.dsp?fullName' Arbitrary File Disclosure |
linux/remote/27[01;31m[K23[m[K3.txt

SAP Business Connector 4.6/4.7 - 'deleteSingle?fullName' Arbitrary File Deletion |
linux/remote/27[01;31m[K23[m[K4.txt

SAP Business One License Manager 2005 - Remote Buffer Overflow (Metasploit) |
windows/remote/164[01;31m[K23[m[K.rb

SAP Internet Transaction Server 4620.2.0.3[01;31m[K23[m[K011 Build 46B.3[01;31m[K23[m[K011 - Cross-Site Scripting |
multiple/remote/[01;31m[K23[m[K071.txt

sap internet transaction server 4620.2.0.3[01;31m[K23[m[K011 build 46b.3[01;31m[K23[m[K011 - Directory Traversal |
multiple/remote/[01;31m[K23[m[K070.txt

SAP Internet Transaction Server 4620.2.0.3[01;31m[K23[m[K011 Build 46B.3[01;31m[K23[m[K011 - Information Disclosure |
multiple/remote/[01;31m[K23[m[K069.txt

SAP SAPCAR - Multiple Vulnerabilities
| linux/dos/40[01;31m[K23[m[K0.txt

Savant Web Server 3.1 - Page Redirect Denial of Service
| windows/dos/[01;31m[K23[m[K191.txt

Savy Soda Documents - Mobile Office Suite '.XLS' Denial of Service
| hardware/dos/138[01;31m[K23[m[K.txt

SBox 1.0.4 - Full Path Disclosure
| cgi/remote/[01;31m[K23[m[K187.txt

ScadaTEC ScadaPhone 5.3.11.1[01;31m[K23[m[K0 - Local Stack Buffer Overflow (Metasploit) |
windows/local/17833.rb

School Event Management System 1.0 - Arbitrary File Upload
| php/webapps/457[01;31m[K23[m[K.txt

SchoolCMS - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K106.txt

Scientific-Atlanta_ Inc. DPR[01;31m[K23[m[K20R2 - Multiple Cross-Site Request Forgery Vulnerabilities |
hardware/webapps/29927.txt

SCO Open Server 5.0.4 - POP Server Buffer Overflow
| linux/remote/191[01;31m[K23[m[K.c

SCO OpenServer 5.0.x - 'mana' 'REMOTE_ADDR' Authentication Bypass
| sco/local/[01;31m[K23[m[K141.sh

SCO OpenServer 5.0.x - 'mana' PATH_INFO Privilege Escalation
| sco/local/[01;31m[K23[m[K143.sh

Scribe 0.2 - 'index.php' Local File Inclusion
| php/webapps/51[01;31m[K23[m[K.txt

Scripts Genie Classified Ultra - SQL Injection / Cross-Site Scripting
| php/webapps/38[01;31m[K23[m[K1.txt

SCRMS 20[01;31m[K23[m[K-05-27 1.0 - Multiple SQL Injection
| php/webapps/51491.txt

Seagate BlackArmor NAS - Privilege Escalation
| hardware/webapps/307[01;31m[K23[m[K.php

Secure Web Gateway 10.2.11 - Cross-Site Scripting (XSS)
| multiple/webapps/51[01;31m[K23[m[K7.txt

Seditio CMS 121 - 'pfs.php' Arbitrary File Upload
| php/webapps/4[01;31m[K23[m[K5.txt

SeedDMS < 5.1.11 - 'out.UsrMgr.php' Cross-Site Scripting
| php/webapps/470[01;31m[K23[m[K.txt

SelectSurvey CMS - 'ASP.NET' Arbitrary File Upload
| asp/webapps/[01;31m[K23[m[K571.txt

Sendmail 8.12.9 - 'Prescan()' Variant Remote Buffer Overrun
| linux/remote/[01;31m[K23[m[K154.c

Sendmail 8.12.x - Header Processing Buffer Overflow (1)
| unix/remote/2[01;31m[K23[m[K13.c

Sendmail 8.12.x - Header Processing Buffer Overflow (2)
| unix/remote/2[01;31m[K23[m[K14.c

Sendmail 8.9.2 - Headers Prescan Denial of Service
| irix/dos/[01;31m[K23[m[K167.c

Sentrifugo 3.2 - File Upload Restriction Bypass
| php/webapps/473[01;31m[K23[m[K.txt

Seo4SMF for SMF forums - Multiple Vulnerabilities
| php/webapps/77[01;31m[K23[m[K.txt

SePortal 2.5 - SQL Injection (2)
| php/remote/3[01;31m[K23[m[K59.txt

Serious Sam Engine 1.0.5 - Remote Denial of Service
| multiple/dos/[01;31m[K23[m[K314.c

Serviio Media Server - checkStreamUrl Command Execution (Metasploit)
| windows/remote/420[01;31m[K23[m[K.rb

Sethi Family Guestbook 3.1.8 - Cross-Site Scripting
| php/webapps/1[01;31m[K23[m[K73.txt

SevOne NMS 5.3.6.0 - Remote Command Execution
| php/webapps/39[01;31m[K23[m[K4.py

Seyeon FlexWATCH Network Video Server 2.2 - Unauthorized Administrative
Access |
hardware/remote/[01;31m[K23[m[K317.txt

Seyeon Technology FlexWATCH Server 2.2 - Cross-Site Scripting
| multiple/remote/[01;31m[K23[m[K756.txt

SFS EZ Pub Site - SQL Injection
| php/webapps/69[01;31m[K23[m[K.txt

SH-HTTPD 0.3/0.4 - Character Filtering Remote Information Disclosure
| linux/remote/[01;31m[K23[m[K295.txt

Shadowed Portal 5.599 - 'root' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K61.txt

Shaun2k2 Palmhttpd Server 3.0 - Remote Denial of Service
| windows/dos/[01;31m[K23[m[K665.c

ShopCartCGI 2.3 - 'gotopage.cgi' Traversal Arbitrary File Access
| cgi/webapps/[01;31m[K23[m[K705.txt

ShopCartCGI 2.3 - genindexpage.cgi Traversal Arbitrary File Access
| cgi/webapps/[01;31m[K23[m[K706.txt

SIEMENS Sipass Integrated 2.6 Ethernet Bus - Arbitrary Pointer
Dereference |
windows/dos/2[01;31m[K23[m[K97.txt

Silentum LoginSys 1.0 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K23[m[K37.txt

Silly Poker 0.25.5 - Local HOME Environment Variable Buffer Overrun
| linux/local/[01;31m[K23[m[K204.c

SilverStripe CMS 3.0.2 - (Multiple Vulnerabilities) Cross-Site
Scripting / Cross-Site Request Forgery |
php/webapps/[01;31m[K23[m[K031.txt

SIMM-Comm SCI Photo Chat 3.4.9 - Directory Traversal
| windows/remote/31[01;31m[K23[m[K1.txt

Simple Chatting System 1.0.0 - Arbitrary File Upload
| php/webapps/43[01;31m[K23[m[K7.txt

Simple Discussion Board 0.1.0 - Remote File Inclusion
| php/webapps/[01;31m[K23[m[K96.txt

Simple Machines Forum (SMF) 1.1 rc2 (Windows) - 'lngfile' Local File
Inclusion |
php/webapps/2[01;31m[K23[m[K1.php

Simple Phone Book 1.0 - 'Username' SQL Injection (Unauthenticated)
| php/webapps/502[01;31m[K23[m[K.txt

Simple Web Server 2.3-rc1 - Directory Traversal
| windows/webapps/[01;31m[K23[m[K886.txt

SimpleBBS 1.0.6 - 'users.php' Insecure File Permissions
| php/webapps/2[01;31m[K23[m[K39.txt

SimpleBlog 2.0 - 'comments.asp' SQL Injection (2)
| php/webapps/2[01;31m[K23[m[K2.pl

SimpleBlog 3.0 - 'comments_get.asp?id' SQL Injection
| asp/webapps/4[01;31m[K23[m[K9.py

SimpleBlog 3.0 - Database Disclosure
| php/webapps/7[01;31m[K23[m[K2.txt

SimplePress CMS 1.0.7 - SQL Injection
| php/webapps/46[01;31m[K23[m[K5.txt

SIPS 0.2.2 - User Information Disclosure
| multiple/remote/2[01;31m[K23[m[K81.txt

SIRCD Server 0.5.2/0.5.3 - Operator Privilege Escalation
| multiple/remote/[01;31m[K23[m[K396.txt

SirsiDynix e-Library 3.5.x - Cross-Site Scripting
| cgi/webapps/46[01;31m[K23[m[K7.txt

```
Site2Nite Auto e-Manager - SQL Injection
| asp/webapps/15[01;31m[K23[m[K0.txt

Site@School 2.4.02 - Arbitrary File Upload
| php/webapps/[01;31m[K23[m[K74.pl

Sitebuilder 1.4 - 'sitebuilder.cgi' Directory Traversal
| cgi/webapps/[01;31m[K23[m[K085.html

SiteEngine 5.x - Multiple Vulnerabilities
| php/webapps/68[01;31m[K23[m[K.txt

Siteframe CMS 2.2.4 - 'download.php' Information Disclosure
| php/webapps/2[01;31m[K23[m[K86.txt

SiteInteractive Subscribe Me - 'Setup.pl' Arbitrary Command Execution
| cgi/webapps/[01;31m[K23[m[K447.txt

SKILLS.com.au Industry App - Man In The Middle Remote Code Execution
| android/remote/4[01;31m[K23[m[K49.txt

Skulltag Huffman 0.97d-beta4.1 - Packet Decompression Remote Heap
Buffer Overflow                          |
multiple/remote/305[01;31m[K23[m[K.txt

Skybluecanvas 1.1 r[01;31m[K23[m[K7 - 'admin.php' Directory Traversal
| php/webapps/34919.txt

Skybluecanvas 1.1 r[01;31m[K23[m[K7 - 'admin.php' Multiple Cross-Site
Scripting Vulnerabilities                        |
php/webapps/34874.txt

Skype for Business 2016 - Cross-Site Scripting
| windows/remote/4[01;31m[K23[m[K16.ps1

Skyvern 0.1.85 - Remote Code Execution (RCE) via SSTI
| multiple/webapps/5[01;31m[K23[m[K35.py

SlimarUSER Management 1.0 - 'id' SQL Injection
| php/webapps/41[01;31m[K23[m[K5.txt

SlimFTPd 3.15 - Remote Buffer Overflow
| windows/remote/6[01;31m[K23[m[K.c

SLocate 2.6 - User-Supplied Database Heap Overflow
| linux/local/[01;31m[K23[m[K228.c

SL_Site 1.0 - 'spaw_root' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K17.txt

SmallFTPd 1.0.3 - Remote Denial of Service
| windows/dos/[01;31m[K23[m[K716.txt
```

```
Smart Search 4.25 - Remote Command Execution
| cgi/webapps/2[01;31m[K23[m[K80.pl

SmartCMS - '/index.php?menuitem' SQL Injection / Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K029.txt

SmarterStats 11.3.6347 - Cross-Site Scripting
| aspx/webapps/429[01;31m[K23[m[K.txt

SmartFTP Client 9.0.26[01;31m[K23[m[K.0 - Denial of Service (PoC)
| windows/dos/45966.py

smartplugs 1.3 - 'showplugs.php' SQL Injection
| php/webapps/116[01;31m[K23[m[K.txt

Smartshop 1 - 'id' SQL Injection
| php/webapps/448[01;31m[K23[m[K.txt

SMC Router 1.2x - Random UDP Packet Denial of Service
| hardware/dos/[01;31m[K23[m[K190.pl

SmodCMS 4.07 (fckeditor) - Arbitrary File Upload
| php/webapps/1[01;31m[K23[m[K76.php

SnapStream PVS Lite 2.0 - Cross-Site Scripting
| windows/remote/[01;31m[K23[m[K529.txt

Snitz Forum v1.0 - Blind SQL Injection
| asp/webapps/513[01;31m[K23[m[K.txt

SnoGrafx - 'cat.php?cat' SQL Injection
| php/webapps/145[01;31m[K23[m[K.txt

Snort 2 - DCE/RPC Preprocessor Buffer Overflow (Metasploit)
| multiple/remote/187[01;31m[K23[m[K.rb

Social Sites MyBB Plugin 0.2.2 - Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K382.txt

Socketwiz BookMarks 2.0 - 'root_dir' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K36.pl

Softalk Mail Server 8.5.1 - 'APPEND' Remote Denial of Service
| multiple/dos/3[01;31m[K23[m[K10.txt

SoftBB 0.1 - 'cmd' Remote Command Execution
| php/webapps/[01;31m[K23[m[K00.pl

Software602 602Pro LAN Suite - Web Mail Cross-Site Scripting
| windows/remote/[01;31m[K23[m[K776.txt

software602 602pro lan suite 2003 - Directory Traversal
| windows/remote/[01;31m[K23[m[K185.txt
```

Software602 602Pro LAN SUITE 2003 - Sensitive User Information Storage
| windows/webapps/[01;31m[K23[m[K184.txt

Solaris 2.7/2.8 Catman - Local Insecure tmp Symlink
| windows/dos/[01;31m[K23[m[K3.pl

Solaris 7.0 - 'cancel' Local Privilege Escalation
| solaris/local/19[01;31m[K23[m[K4.c

Solaris 7.0 - 'chkperm' Local Privilege Escalation
| solaris/local/19[01;31m[K23[m[K5.txt

Solaris 7.0 - 'Coredump' File Write
| solaris/remote/19[01;31m[K23[m[K6.txt

Solaris 7.0 - aspppd Insecure Temporary File Creation
| solaris/local/19[01;31m[K23[m[K3.txt

Solaris 8 dtspcd - Remote Heap Overflow (Metasploit)
| solaris/remote/99[01;31m[K23[m[K.rb

Solaris dtspcd - Remote Heap Overflow (Metasploit)
| solaris_sparc/remote/163[01;31m[K23[m[K.rb

SolarWinds Serv-U 15.4.2 HF1 - Directory Traversal
| multiple/remote/5[01;31m[K23[m[K11.py

Somery 0.4.6 - 'skin_dir' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K29.txt

Sonicwall < 8.1.0.2-14sv - 'sitecustomization.cgi' Command Injection
(Metasploit) |
cgi/webapps/4[01;31m[K23[m[K44.rb

Sonicwall < 8.1.0.6-21sv - 'gencsr.cgi' Command Injection (Metasploit)
| cgi/webapps/4[01;31m[K23[m[K43.rb

Sonicwall Secure Remote Access 8.1.0.2-14sv - Command Injection
| cgi/webapps/4[01;31m[K23[m[K42.txt

SonicWALL SonicOS 5.8.1.8 WAF - Cross-Site Scripting
| hardware/webapps/[01;31m[K23[m[K498.txt

Sonique2 2.0 Beta Build 103 - Local Crash (PoC)
| windows/dos/11[01;31m[K23[m[K4.py

Sony PC Companion 2.1 - 'Admin_RemoveDirectory()' Unicode Stack Buffer
Overflow |
windows/dos/[01;31m[K23[m[K569.txt

Sony PC Companion 2.1 - 'CheckCompatibility()' Unicode Stack Buffer
Overflow |
windows/dos/[01;31m[K23[m[K568.txt

Sony PC Companion 2.1 - 'DownloadURLToFile()' Unicode Stack Buffer Overflow | windows/dos/[01;31m[K23[m[K565.txt

Sony PC Companion 2.1 - 'Load()' Unicode Stack Buffer Overflow | windows/dos/[01;31m[K23[m[K567.txt

Sophos Anti-Virus 3.x - Reserved MS-DOS Name Scan Evasion | windows/remote/246[01;31m[K23[m[K.txt

Sophos Web Appliance 4.3.0.2 - 'trafficType' Remote Command Injection (Metasploit) | json/webapps/4[01;31m[K23[m[K32.rb

Sound eXchange (SoX) 14.4.2 - Multiple Vulnerabilities | linux/dos/4[01;31m[K23[m[K98.txt

SoundTouch 1.9.2 - Multiple Vulnerabilities | linux/dos/4[01;31m[K23[m[K89.txt

SourceForge 1.0.4 - 'database.php' Remote File Inclusion | php/webapps/26[01;31m[K23[m[K.pl

South River Technologies WebDrive 9.02 build 2[01;31m[K23[m[K2 - Local Privilege Escalation | windows/local/9970.txt

South River Technologies WebDrive Service 9.02 build 2[01;31m[K23[m[K2 - Bad Security Descriptor Privilege Escalation | windows/local/11264.rb

Speed Commander 13.10 - '.zip' Memory Corruption | windows/dos/1[01;31m[K23[m[K14.py

Sphider Search Engine - Multiple Vulnerabilities | php/webapps/34[01;31m[K23[m[K8.txt

SPHPBlog 0.4 - 'search.php' Cross-Site Scripting | php/webapps/254[01;31m[K23[m[K.txt

SpiderSales 2.0 Shopping Cart - Multiple Vulnerabilities | asp/webapps/[01;31m[K23[m[K791.txt

SPIP CMS < 2.0.[01;31m[K23[m[K/ 2.1.22/3.0.9 - Privilege Escalation | php/webapps/33425.py

Splunk 5.0 - Custom App Remote Code Execution (Metasploit) | multiple/remote/[01;31m[K23[m[K224.rb

Splunk Enterprise 7.2.3 - (Authenticated) Custom App Remote Code Execution | windows/webapps/46[01;31m[K23[m[K8.py

```
Sponge News 2.2 - 'sndir' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K09.txt

SpotAuditor 5.3.2 - 'Key' Denial of Service
| windows/dos/477[01;31m[K23[m[K.py

Spy Emergency [01;31m[K23[m[K.0.205 - Unquoted Service Path Privilege
Escalation                                          |
windows/local/40550.txt

SpyCamLizard 1.[01;31m[K23[m[K0 - Denial of Service
| windows/dos/41667.py

SpyCamLizard 1.[01;31m[K23[m[K0 - Remote Buffer Overflow
| windows/remote/42222.py

SQLiteWebAdmin 0.1 - 'tpl.inc.php' Remote File Inclusion
| php/webapps/21[01;31m[K23[m[K.txt

Squid Proxy 2.4/2.5 - NULL URL Character Unauthorized Access
| linux/remote/[01;31m[K23[m[K777.txt

SquidGuard 1.x - NULL URL Character Unauthorized Access
| linux/remote/[01;31m[K23[m[K848.txt

Srcpd 2.0 - Multiple Buffer Overflow Vulnerabilities
| linux/remote/[01;31m[K23[m[K049.c

Srcpd 2.0 - Remote Integer Overflow
| linux/dos/[01;31m[K23[m[K048.txt

Standard & Poors ComStock 4.2.4 - Command Execution
| unix/local/198[01;31m[K23[m[K.txt

Status2k Server Monitoring Software - Multiple Vulnerabilities
| php/webapps/34[01;31m[K23[m[K9.txt

Steam Windows Client - Local Privilege Escalation
| windows/local/47[01;31m[K23[m[K8.ps1

Stellar Docs 1.2 - Full Path Disclosure
| php/webapps/[01;31m[K23[m[K009.txt

Strapi 3.0.0-beta - Set Password (Unauthenticated)
| multiple/webapps/50[01;31m[K23[m[K7.py

Strapi 3.0.0-beta.17.7 - Remote Code Execution (RCE) (Authenticated)
| multiple/webapps/50[01;31m[K23[m[K8.py

Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE)
(Unauthenticated)                                   |
multiple/webapps/50[01;31m[K23[m[K9.py
```

StreamAudio ChainCast ProxyManager - 'ccpm_0[01;31m[K23[m[K7.dll' Remote Buffer Overflow | windows/remote/4894.html

Stylemotion WEB//NEWS 1.4 - 'news.php' Multiple SQL Injections | php/webapps/26[01;31m[K23[m[K5.txt

Stylemotion WEB//NEWS 1.4 - 'print.php?id' SQL Injection | php/webapps/26[01;31m[K23[m[K6.txt

Stylemotion WEB//NEWS 1.4 - 'startup.php' Cookie SQL Injection | php/webapps/26[01;31m[K23[m[K4.txt

Subberz Lite - UserFunc Remote File Inclusion | php/webapps/282[01;31m[K23[m[K.txt

Subdreamer 1.0 - SQL Injection | php/webapps/25[01;31m[K23[m[K5.txt

SugarCRM 6.5.[01;31m[K23[m[K - REST PHP Object Injection (Metasploit) | php/remote/40344.rb

sugarsales 1.x/2.0 - Multiple Vulnerabilities | php/webapps/248[01;31m[K23[m[K.txt

Sumatra PDF 1.1 - Denial of Service | windows/dos/34[01;31m[K23[m[K3.py

SumatraPDF 2.1.1/MuPDF 1.0 - Integer Overflow | windows/dos/[01;31m[K23[m[K246.txt

Sun Cobalt RaQ 1.1/2.0/3.0/4.0 - 'Message.cgi' Cross-Site Scripting | cgi/webapps/[01;31m[K23[m[K214.txt

Sun J2EE/RI 1.4 / Sun JDK 1.4.2 - JDBC Database Insecure Default Policy | windows/remote/[01;31m[K23[m[K552.xml

Sun Java 1.x - XML Document Nested Entity Denial of Service | windows/dos/[01;31m[K23[m[K165.txt

Sun Java Plugin 1.4 - Unauthorized Java Applet Floppy Access | windows/remote/[01;31m[K23[m[K270.java

Sun Java Plugin 1.4.2 _01 - Cross-Site Applet Sandbox Security Model Violation | windows/remote/[01;31m[K23[m[K265.txt

Sun Java Virtual Machine 1.x - Slash Path Security Model Circumvention | multiple/dos/[01;31m[K23[m[K276.java

Sun Java Web Server 7.0 u7 - Admin Interface Denial of Service | windows/dos/14[01;31m[K23[m[K6.txt

Sun JDK/SDK 1.3/1.4 / IBM JDK 1.3.1 / BEA Systems WebLogic 5/6/7 - java.util.zip Null Value Denial of Serv | multiple/dos/2[01;31m[K23[m[K58.cfm

Sun JDK/SDK 1.3/1.4 / IBM JDK 1.3.1 / BEA Systems WebLogic 5/6/7 - java.util.zip Null Value Denial of Serv | multiple/dos/2[01;31m[K23[m[K59.xsl

Sun JDK/SDK 1.3/1.4 / IBM JDK 1.3.1 / BEA Systems WebLogic 5/6/7 - java.util.zip Null Value Denial of Serv | multiple/dos/2[01;31m[K23[m[K60.java

Sun Management Center 3.0/3.5 - Error Message Information Disclosure | solaris/remote/[01;31m[K23[m[K272.txt

Sun Microsystems Java Virtual Machine 1.x - Security Manager Denial of Service | multiple/dos/[01;31m[K23[m[K292.java

Sun Solaris 10 RPC dmispd - Denial of Service | solaris/dos/98[01;31m[K23[m[K.c

Sun Solaris 2.6/7.0/8/9 - vfs_getvfssw function Privilege Escalation | solaris/local/[01;31m[K23[m[K874.txt

Sun Solaris 9/10 Text Editors - Command Execution | solaris/remote/3[01;31m[K23[m[K93.txt

Sun xVM VirtualBox 2.2 < 3.0.2 r49928 - Local Host Reboot (Denial of Service) (PoC) | multiple/dos/93[01;31m[K23[m[K.txt

SunByte e-Flower - 'id' SQL Injection | php/webapps/73[01;31m[K23[m[K.txt

SunOS 4.1.4 - arp(8c) Memory Dump | solaris/local/19[01;31m[K23[m[K2.txt

SunOS 5.7 Catman - Local Insecure tmp Symlink Clobber | solaris/dos/[01;31m[K23[m[K5.pl

Supasite 1.[01;31m[K23[m[Kb - Multiple Remote File Inclusions | php/webapps/3771.txt

superlink script 1.0 - 'id' SQL Injection | php/webapps/109[01;31m[K23[m[K.txt

Supply Chain Management System - Auth Bypass SQL Injection | php/webapps/49[01;31m[K23[m[K9.txt

SureCom EP-9510AX/EP-4504AX Network Device - Malformed Web Authorisation Request Denial of Service (1) | hardware/dos/[01;31m[K23[m[K788.pl

SureCom EP-9510AX/EP-4504AX Network Device - Malformed Web Authorisation Request Denial of Service (2) | hardware/dos/[01;31m[K23[m[K789.c

Surfboard HTTPd 1.1.9 - Remote Buffer Overflow (PoC) | windows/dos/[01;31m[K23[m[K480.txt

Surfnet 1.31 - CMD_CREDITCARD_CHARGE Denial of Service | windows/dos/[01;31m[K23[m[K512.txt

Surfnet 1.31 - Unauthorized Account Depositing | windows/local/[01;31m[K23[m[K511.txt

SurgeFTP [01;31m[K23[m[Kb6 - Multiple Cross-Site Scripting Vulnerabilities | cgi/remote/36045.txt

SurgeLDAP 1.0 - 'User.cgi' Directory Traversal | cgi/remote/[01;31m[K23[m[K987.txt

SurgeLDAP 1.0 d - 'User.cgi' Cross-Site Scripting | cgi/webapps/[01;31m[K23[m[K025.txt

SurgeLDAP 1.0 d - Full Path Disclosure | multiple/remote/[01;31m[K23[m[K024.txt

SuSE Linux 6.3/6.4 - Installed Package Disclosure | linux/remote/20[01;31m[K23[m[K6.txt

SuSE Linux Professional 8.2 - SuSEWM Configuration File Insecure Temporary File | linux/local/[01;31m[K23[m[K2[01;31m[K23[m[K.c

SWSoft Confixx 3.1.2 - 'Jahr' Cross-Site Scripting | php/webapps/276[01;31m[K23[m[K.txt

SX Design sipd 0.1.2 - Remote Denial of Service | multiple/dos/[01;31m[K23[m[K431.pl

SX Design sipd 0.1.2/0.1.4 - Remote Format String | multiple/dos/[01;31m[K23[m[K444.pl

Sygate Personal Firewall 5.0 - DLL Authentication Bypass | windows/remote/[01;31m[K23[m[K489.txt

Symantec Client Firewall Products 5 - 'SYMNDIS.SYS' Driver Remote Denial of Service | windows/dos/[01;31m[K23[m[K846.txt

Symantec Endpoint Protection 12.1.40[01;31m[K23[m[K.4080 - Multiple Vulnerabilities | jsp/webapps/35181.txt

```
Symantec Gateway Security 5400 Series 2.0 - Error Page Cross-Site
Scripting                                  |
hardware/remote/[01;31m[K23[m[K764.txt

Symantec Messaging Gateway 9.5.3-3 - Arbitrary File Download
| linux/webapps/[01;31m[K23[m[K110.txt

Symantec Messaging Gateway 9.5.3-3 - Cross-Site Request Forgery
| multiple/webapps/[01;31m[K23[m[K109.txt

Symantec Norton Internet Security 2003 6.0.4.34 - Error Message Cross-
Site Scripting                          |
cgi/remote/[01;31m[K23[m[K304.txt

Symantec pcAnywhere - Insecure File Permissions Privilege Escalation
| windows/local/188[01;31m[K23[m[K.txt

Symantec PCAnywhere32 8.0 - Denial of Service
| multiple/dos/19[01;31m[K23[m[K0.txt

Symantec Security Check Virus Detection - COM Object Denial of Service
| windows/dos/[01;31m[K23[m[K919.txt

Symantec Web Gateway 5.0.3.18 - 'deptUploads_data.php?groupid' Blind
SQL Injection                           |
php/webapps/201[01;31m[K23[m[K.py

Sync Breeze 13.6.18 - 'Multiple' Unquoted Service Path
| windows/local/500[01;31m[K23[m[K.txt

Sync Breeze Enterprise 10.0.28 - Remote Buffer Overflow (PoC)
| windows/dos/4[01;31m[K23[m[K41.c

Sync Breeze Server 2.2.30 - Remote Buffer Overflow
| windows/remote/15[01;31m[K23[m[K1.py

Synthetic Reality SymPoll 1.5 - Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K330.txt

systemd (systemd-tmpfiles) < [01;31m[K23[m[K6 -
'fs.protected_hardlinks=0' Local Privilege Escalation
| linux/local/43935.txt

Systrace 1.x - Local Policy Bypass
| linux/local/[01;31m[K23[m[K892.c

Talkie Bluetooth Video iFiles 2.0 iOS - Multiple Vulnerabilities
| ios/webapps/28[01;31m[K23[m[K6.txt

Targem Games Battle Mages 1.0 - Remote Denial of Service
| multiple/dos/[01;31m[K23[m[K805.txt
```

Target Longlife Media Player 2.0.2.0 - '.wav' Crash (PoC)
| windows/dos/28[01;31m[K23[m[K7.py

Task Management System 1.0 - Unrestricted File Upload to Remote Code Execution |
php/webapps/492[01;31m[K23[m[K.txt

TCExam 11.1.29 - 'tce_xml_user_results.php' Multiple SQL Injections
| php/webapps/357[01;31m[K23[m[K.txt

TCLhttpd 3.4.2 - Directory Listing Disclosure
| multiple/remote/[01;31m[K23[m[K173.txt

TCLHttpd 3.4.2 - Multiple Cross-Site Scripting Vulnerabilities
| multiple/remote/[01;31m[K23[m[K174.txt

TCPDump 3.6/3.7 - Malformed RADIUS Packet Denial of Service
| linux/dos/2[01;31m[K23[m[K52.txt

Tcpdump 3.x - L2TP Parser Remote Denial of Service
| linux/dos/[01;31m[K23[m[K452.txt

TeamCal Pro 2.8.001 - 'app_root' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K68.txt

TeamSpeak 2.0.[01;31m[K23[m[K.17 - Remote File Disclosure
| multiple/remote/7760.php

TeamSpeak Server 2.0.[01;31m[K23[m[K (Multiple Scripts) - Multiple Cross-Site Scripting Vulnerabilities |
multiple/remote/30025.txt

TeamViewer 5.0.8[01;31m[K23[m[K2 - Remote Buffer Overflow
| windows/remote/34002.c

Techno Dreams Articles & Papers 2.0 - SQL Injection
| asp/webapps/[01;31m[K23[m[K86.txt

Techno Dreams FAQ Manager 1.0 - SQL Injection
| asp/webapps/[01;31m[K23[m[K85.txt

Technote 2000/2001 - 'Filename' Command Execution / File Disclosure
| cgi/remote/205[01;31m[K23[m[K.pl

Tekman Portal 1.0 - 'tr' SQL Injection
| asp/webapps/[01;31m[K23[m[K95.txt

TelCondex SimpleWebserver 2.12.30210 build 3285 - HTTP Referer Remote Buffer Overflow |
windows/dos/[01;31m[K23[m[K310.pl

TelCondex SimpleWebserver 2.13.31027 build 3289 - Directory Traversal
| windows/remote/[01;31m[K23[m[K365.txt

```
Telekorn Signkorn Guestbook 1.3 - 'dir_path' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K54.txt

Telekorn Signkorn Guestbook 1.x - '/includes/functions.gb.php?dir_path'
Remote File Inclusion              | php/webapps/285[01;31m[K23[m[K.txt

telepark wiki 2.4.[01;31m[K23[m[K - Multiple Vulnerabilities
| php/webapps/10101.txt

Tellurian TftpdNT 1.8/2.0 - 'Filename' Buffer Overrun
| windows/remote/[01;31m[K23[m[K066.pl

Template Seller Pro 3.25 - 'tempid' SQL Injection
| php/webapps/1[01;31m[K23[m[K60.pl

TerminatorX 3.8 - Multiple Command-Line and Environment Buffer Overrun
Vulnerabilities (1)                | linux/local/[01;31m[K23[m[K350.c

TerminatorX 3.8 - Multiple Command-Line and Environment Buffer Overrun
Vulnerabilities (2)                | linux/local/[01;31m[K23[m[K351.c

TerminatorX 3.8 - Multiple Command-Line and Environment Buffer Overrun
Vulnerabilities (3)                | linux/local/[01;31m[K23[m[K352.c

Testa 3.5.1 Online Test Management System - Reflected Cross-Site
Scripting (XSS)                                 |
php/webapps/510[01;31m[K23[m[K.txt

Texas Imperial Software WFTPD 3.[01;31m[K23[m[K - 'SIZE' Remote Buffer
Overflow                                          |
windows/remote/2[01;31m[K23[m[K3.c

Texas Imperial Software WFTPD 3.[01;31m[K23[m[K - SIZE Overflow
(Metasploit)                                                |
windows/remote/16741.rb

Textpad 7.6.4 - Denial Of Service (PoC)
| windows_x86/dos/45[01;31m[K23[m[K8.py

textpattern CMS 4.2.0 - Remote File Inclusion
| php/webapps/148[01;31m[K23[m[K.txt

Textpattern CMS v4.8.8 - Stored Cross-Site Scripting (XSS)
(Authenticated)                                     |
php/webapps/515[01;31m[K23[m[K.txt

TGS Content Management 0.3.2r2 - 'login.php' Multiple Cross-Site
Scripting Vulnerabilities                  |
php/webapps/320[01;31m[K23[m[K.txt

The Includer CGI 1.0 - Remote Command Execution (3)
| cgi/webapps/9[01;31m[K23[m[K.pl
```

```
ThinkPHP 5.0.[01;31m[K23[m[K/5.1.31 - Remote Code Execution
| php/webapps/45978.txt

Thomson Cablemodem TCM315 - Denial of Service
| hardware/dos/[01;31m[K23[m[K394.c

Thomson Reuters Fixed Assets CS 13.1.4 - Local Privilege Escalation
| windows/local/354[01;31m[K23[m[K.txt

thttpd 2.2x - 'defang' Remote Buffer Overflow
| linux/remote/[01;31m[K23[m[K306.c

thttpd 2.2x - 'defang' Remote Buffer Overflow (PoC)
| linux/dos/[01;31m[K23[m[K305.c

Thunderstone TEXIS 3.0 - 'texis.exe' Information Disclosure
| cgi/remote/2[01;31m[K23[m[K55.txt

TightVNC 2.8.83 - Control Pipe Manipulation
| multiple/local/5[01;31m[K23[m[K22.c

TikiWiki Project 1.8 - 'categorize.php' Direct Request Full Path
Disclosure                                |
php/webapps/[01;31m[K23[m[K952.txt

TikiWiki Project 1.8 - 'img/wiki_up' Arbitrary File Upload
| php/webapps/[01;31m[K23[m[K948.txt

TikiWiki Project 1.8 - 'messu-mailbox.php' Multiple Cross-Site
Scripting Vulnerabilities                  |
php/webapps/[01;31m[K23[m[K953.txt

TikiWiki Project 1.8 - 'messu-read.php' Multiple Cross-Site Scripting
Vulnerabilities                       |
php/webapps/[01;31m[K23[m[K954.txt

TikiWiki Project 1.8 - 'tiki-browse_categories.php?parentId' Cross-Site
Scripting                           | php/webapps/[01;31m[K23[m[K956.txt

TikiWiki Project 1.8 - 'tiki-browse_categories.php?sort_mode' SQL
Injection                                 |
php/webapps/[01;31m[K23[m[K966.txt

TikiWiki Project 1.8 - 'tiki-directory_ranking.php?sort_mode' SQL
Injection                                 |
php/webapps/[01;31m[K23[m[K965.txt

TikiWiki Project 1.8 - 'tiki-directory_search.php?sort_mode' SQL
Injection                                  |
php/webapps/[01;31m[K23[m[K973.txt
```

TikiWiki Project 1.8 - 'tiki-file_galleries.php?sort_mode' SQL Injection |
php/webapps/[01;31m[K23[m[K974.txt

TikiWiki Project 1.8 - 'tiki-index.php?comments_offset & offset' SQL Injections |
php/webapps/[01;31m[K23[m[K971.txt

TikiWiki Project 1.8 - 'tiki-index.php?comments_threshold' Cross-Site Scripting |
php/webapps/[01;31m[K23[m[K957.txt

TikiWiki Project 1.8 - 'tiki-list_blogs.php?offset' SQL Injection
| php/webapps/[01;31m[K23[m[K984.txt

TikiWiki Project 1.8 - 'tiki-list_blogs.php?sort_mode' SQL Injection
| php/webapps/[01;31m[K23[m[K977.txt

TikiWiki Project 1.8 - 'tiki-list_faqs.php?offset' SQL Injection
| php/webapps/[01;31m[K23[m[K982.txt

TikiWiki Project 1.8 - 'tiki-list_faqs.php?sort_mode' SQL Injection
| php/webapps/[01;31m[K23[m[K975.txt

TikiWiki Project 1.8 - 'tiki-list_file_gallery.php?galleryID' Cross-Site Scripting |
php/webapps/[01;31m[K23[m[K959.txt

TikiWiki Project 1.8 - 'tiki-list_file_gallery.php?sort_mode' SQL Injection |
php/webapps/[01;31m[K23[m[K964.txt

TikiWiki Project 1.8 - 'tiki-list_trackers.php?offset' SQL Injection
| php/webapps/[01;31m[K23[m[K983.txt

TikiWiki Project 1.8 - 'tiki-list_trackers.php?sort_mode' SQL Injection
| php/webapps/[01;31m[K23[m[K976.txt

TikiWiki Project 1.8 - 'tiki-map.phtml' Traversal Arbitrary File / Directory Enumeration |
php/webapps/[01;31m[K23[m[K949.txt

TikiWiki Project 1.8 - 'tiki-print_article.php?articleId' Cross-Site Scripting |
php/webapps/[01;31m[K23[m[K958.txt

TikiWiki Project 1.8 - 'tiki-read_article.php?articleId' Cross-Site Scripting |
php/webapps/[01;31m[K23[m[K955.txt

TikiWiki Project 1.8 - 'tiki-switch_theme.php?theme' Cross-Site Scripting |
php/webapps/[01;31m[K23[m[K947.txt

TikiWiki Project 1.8 - 'tiki-upload_file.php?galleryID' Cross-Site Scripting |
php/webapps/[01;31m[K23[m[K960.txt

TikiWiki Project 1.8 - 'tiki-usermenu.php?offset' SQL Injection
| php/webapps/[01;31m[K23[m[K978.txt

TikiWiki Project 1.8 - 'tiki-usermenu.php?sort_mode' SQL Injection
| php/webapps/[01;31m[K23[m[K963.txt

TikiWiki Project 1.8 - 'tiki-user_tasks.php?offset & sort_mode' SQL Injections |
php/webapps/[01;31m[K23[m[K972.txt

TikiWiki Project 1.8 - 'tiki-view_chart.php?chartId' Cross-Site Scripting |
php/webapps/[01;31m[K23[m[K962.txt

TikiWiki Project 1.8 - 'tiki-view_faq.php?faqId' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K961.txt

TikiWiki Project 1.8 - Add Site Multiple Options Remote Code Injections
| php/webapps/[01;31m[K23[m[K951.txt

TikiWiki Project 1.8 - User Profile Multiple Option Remote Code Injections |
php/webapps/[01;31m[K23[m[K950.txt

Tilde CMS 1.01 - Multiple Vulnerabilities
| php/webapps/4[01;31m[K23[m[K48.txt

Time and Expense Management System - Multiple Vulnerabilities
| php/webapps/17[01;31m[K23[m[K9.txt

TinyPHPForum 3.6 - 'UpdatePF.php' Authentication Bypass
| php/webapps/283[01;31m[K23[m[K.txt

TinyServer 1.1 - Cross-Site Scripting
| windows/remote/[01;31m[K23[m[K596.txt

TinyServer 1.1 - Denial of Service
| windows/dos/[01;31m[K23[m[K595.txt

tinyserver 1.1 - Directory Traversal
| windows/remote/[01;31m[K23[m[K594.txt

TIPS MailPost 5.1.1 - Remote File Enumeration
| cgi/webapps/247[01;31m[K23[m[K.txt

TipsOfTheDay MyBB Plugin - Multiple Vulnerabilities
| php/webapps/[01;31m[K23[m[K322.txt

```
Tlen.pl 5.[01;31m[K23[m[K.4.1 - Instant Messenger Remote Script
Execution                                                 |
cgi/webapps/25042.txt

Toko Instan 7.6 - Multiple SQL Injections
| php/webapps/46[01;31m[K23[m[K.txt

Tolis Group BRU 17.0 - Local Privilege Escalation (1)
| unix/local/229[01;31m[K23[m[K.c

Toshiba e-Studio (Multiple Devices) - Security Bypass
| multiple/remote/36[01;31m[K23[m[K8.txt

TOSHIBA e-Studio [01;31m[K23[m[K2/[01;31m[K23[m[K3/282/283 - Cross-Site
Request Forgery (Change Admin Password)                   |
hardware/webapps/29570.txt

Total Video Player 1.3.7 - '.m3u' Local Buffer Overflow
| windows/local/79[01;31m[K23[m[K.c

Totem Movie Player 3.4.3 (Ubuntu) - Stack Corruption
| linux/dos/[01;31m[K23[m[K427.txt

Tourism Management System v2.0 - Arbitrary File Upload
| php/webapps/519[01;31m[K23[m[K.txt

Tower Toppler 0.99.1 - 'Display' Local Buffer Overflow
| unix/local/2[01;31m[K23[m[K35.pl

TP-Link TD-W8950ND ADSL2+ - Remote DNS Change
| hardware/webapps/37[01;31m[K23[m[K8.txt

TP-Link TL-MR3220 - Cross-Site Scripting
| hardware/webapps/430[01;31m[K23[m[K.txt

TR Forum 1.5 - Cross-Site Request Forgery (Add Admin)
| php/webapps/1[01;31m[K23[m[K85.html

TrackerCam 5.12 - 'ComGetLogFile.php3?fm' Traversal Arbitrary File
Access                                    |
php/webapps/251[01;31m[K23[m[K.txt

Tracks 1.7.2 - URI Cross-Site Scripting
| php/webapps/355[01;31m[K23[m[K.txt

Tradingeye E-Commerce Shopping Cart - Multiple Vulnerabilities
| php/webapps/175[01;31m[K23[m[K.txt

TransSoft Broker FTP Server 6.1 - Denial of Service
| windows/dos/[01;31m[K23[m[K715.pl

Traq 2.3 - Authentication Bypass / Remote Code Execution (Metasploit)
| php/webapps/18[01;31m[K23[m[K9.rb
```

```
Travel411 - SQL Injection
| php/webapps/17[01;31m[K23[m[K6.txt

Trend Micro Interscan VirusWall localweb - Directory Traversal
| windows/webapps/[01;31m[K23[m[K875.txt

TRENDnet TEW-634GRU 1.00.[01;31m[K23[m[K - Multiple Vulnerabilities
| hardware/webapps/33090.txt

Tridia DoubleVision 3.0 7.00 - Local Privilege Escalation
| sco/local/20[01;31m[K23[m[K0.c

Trillian 0.74 - IRC Oversized Data Block Buffer Overflow
| windows/dos/218[01;31m[K23[m[K.c

Tritanium Scripts Tritanium Bulletin Board 1.2.3 - Unauthorized Access
| php/webapps/[01;31m[K23[m[K319.txt

TRN Threaded USENET News Reader 3.6-[01;31m[K23[m[K - Local Stack
Overflow                                                  |
linux/local/39764.py

Trouble Ticket Express 3.01 - Remote Code Execution / Directory
Traversal                                    |
cgi/webapps/117[01;31m[K23[m[K.pl

Trouble Ticket Software - 'ttx.cgi' Arbitrary File Download
| cgi/webapps/118[01;31m[K23[m[K.txt

TSguestbook 2.1 - 'Message' HTML Injection
| php/webapps/[01;31m[K23[m[K084.txt

TSOKA:CMS 1.1/1.9/2.0 - SQL Injection / Cross-Site Scripting
| php/webapps/119[01;31m[K23[m[K.txt

TualBLOG 1.0 - 'icerikno' SQL Injection
| asp/webapps/[01;31m[K23[m[K62.txt

Tuniac 1007[01;31m[K23[m[K - Denial of Service
| windows/dos/14689.pl

Turbo FTP Server 1.30.8[01;31m[K23[m[K - PORT Overflow (Metasploit)
| windows/remote/22161.rb

Tutorialms 1.4 - 'show' SQL Injection
| php/webapps/171[01;31m[K23[m[K.txt

Tutos 1.1.20031017 - 'note_overview.php?id' SQL Injection
| php/webapps/[01;31m[K23[m[K991.txt

TVMOBiLi 2.1.0.3557 - Denial of Service
| windows/dos/[01;31m[K23[m[K254.txt
```

```
TVT TD-[01;31m[K23[m[K08SS-B DVR - Directory Traversal
| hardware/webapps/29959.txt

TWiki MAKETEXT - Remote Command Execution (Metasploit)
| unix/remote/[01;31m[K23[m[K579.rb

Twitter-Clone 1 - 'userid' SQL Injection
| php/webapps/45[01;31m[K23[m[K0.txt

Twitter-Clone 1 - Cross-Site Request Forgery (Delete Post)
| php/webapps/45[01;31m[K23[m[K2.txt

Typo3 3.5 b5 - HTML Hidden Form Field Information Disclosure (1)
| php/webapps/2[01;31m[K23[m[K15.pl

Typo3 3.5 b5 - HTML Hidden Form Field Information Disclosure (2)
| php/webapps/2[01;31m[K23[m[K16.pl

TYPSoft FTP Server 1.1 - Remote CPU Consumption (Denial of Service)
| windows/dos/[01;31m[K23[m[K731.txt

TYPSoft FTP Server 1.10 - APPE DELE Denial of Service
| windows/dos/102[01;31m[K23[m[K.txt

UBBCentral UBB.Threads 7.3.1 - 'Forum[]' Array SQL Injection
| php/webapps/3[01;31m[K23[m[K47.txt

Ubee EVW3200 - Cross-Site Request Forgery
| hardware/webapps/32[01;31m[K23[m[K8.txt

Ubee EVW3200 - Multiple Persistent Cross-Site Scripting Vulnerabilities
| hardware/webapps/32[01;31m[K23[m[K7.txt

Ubiquiti AirOS 5.5.2 - (Authenticated) Remote Command Execution
| hardware/remote/[01;31m[K23[m[K735.py

Ubisoft CoGSManager ActiveX Control 1.0.0.[01;31m[K23[m[K -
'Initialize()' Method Stack Buffer Overflow                |
windows/remote/35885.txt

UC Gateway Investment SiteEngine 5.0 - 'api.php' Open Redirection
| php/webapps/325[01;31m[K23[m[K.txt

Uiga Personal Portal - 'index.php' 'view' SQL Injection
| php/webapps/1[01;31m[K23[m[K99.txt

Ulicms 20[01;31m[K23[m[K.1 - create admin user via mass assignment
| php/webapps/51486.txt

Ulicms-20[01;31m[K23[m[K.1 sniffing-vicuna - Remote Code Execution
(RCE)                                                      |
php/webapps/51434.txt
```

```
Ulicms-20[01;31m[K23[m[K.1 sniffing-vicuna - Stored Cross-Site
Scripting (XSS)                                          |
php/webapps/51435.txt

Ulicms-20[01;31m[K23[m[K.1-sniffing-vicuna - Privilege escalation
| php/webapps/51433.py

Ultimate Locator - 'radius' SQL Injection
| php/webapps/366[01;31m[K23[m[K.txt

Ultimate PHP Board 1.0/1.1 - Image Tag Script Injection
| php/webapps/214[01;31m[K23[m[K.txt

UltraISO 9.7.1.3519 - Denial Of Service (PoC)
| windows_x86-64/dos/45[01;31m[K23[m[K9.py

UMPlayer Portable 0.95 - Crash (PoC)
| windows/dos/[01;31m[K23[m[K003.py

UNAK-CMS 1.5 - 'dirroot' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K80.txt

Unreal Engine - 'UnChan.cpp' Failed Assertion Remote Denial of Service
| multiple/dos/3[01;31m[K23[m[K86.txt

Unreal Engine 3 - Failed Memory Allocation Remote Denial of Service
| multiple/dos/3[01;31m[K23[m[K62.txt

UoW IMAPd Serve 10.[01;31m[K23[m[K4/12.264 - COPY Buffer Overflow
(Metasploit)                                             |
unix/remote/19849.pm

UoW IMAPd Server 10.[01;31m[K23[m[K4/12.264 - LSUB Buffer Overflow
(Metasploit)                                            |
unix/remote/19848.pm

UoW IMAPd Server 10.[01;31m[K23[m[K4/12.264 - Remote Buffer Overflow
| unix/remote/19847.c

UoW Pine 4.0.4/4.10/4.21 - 'From:' Remote Buffer Overflow
| linux/remote/20[01;31m[K23[m[K7.c

Uploader by CeleronDude 5.3.0 - Arbitrary File Upload (1)
| php/webapps/105[01;31m[K23[m[K.txt

UranyumSoft Ýlan Servisi - Database Disclosure
| asp/webapps/108[01;31m[K23[m[K.txt

URL Hunter - Local Buffer Overflow (DEP Bypass)
| windows/local/193[01;31m[K23[m[K.c
```

```
UseBB 1.0.7 - '/install/upgrade-0-2-3.php?PHP_SELF' Cross-Site
Scripting                                    |
php/webapps/303[01;31m[K23[m[K.txt

Usermin 1.820 - Remote Code Execution (RCE) (Authenticated)
| linux/webapps/50[01;31m[K23[m[K4.py

uWSGI < 2.0.17 - Directory Traversal
| php/webapps/442[01;31m[K23[m[K.txt

v2marketplacescript Upload_images Script (-7777) - Arbitrary File
Upload                                      |
php/webapps/1[01;31m[K23[m[K15.txt

VACRON VIG-US731VE 1.0.18-09-B727 IP Camera - Authentication Bypass
| hardware/webapps/4[01;31m[K23[m[K52.txt

Valve Software Half-Life Dedicated Server 3.1/4.1 - Information
Disclosure/Denial of Service                |
windows/dos/[01;31m[K23[m[K388.txt

vam shop 1.69 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K23[m[K72.txt

Vastal I-Tech Cosmetics Zone - 'view_products.php' SQL Injection
| php/webapps/33[01;31m[K23[m[K9.txt

vbPortal 2.0 alpha 8.1 - (Authenticated) SQL Injection
| php/webapps/[01;31m[K23[m[K140.txt

VBScript - 'OLEAUT32!VariantClear' and 'scrrun!VBADictionary::put_Item'
Use-After-Free                          |
windows/dos/459[01;31m[K23[m[K.html

VBScript - MSXML Execution Policy Bypass
| windows/dos/460[01;31m[K23[m[K.txt

vBulletin 1.0/1.1/2.0.x/2.2.x - Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K688.txt

vBulletin 2.x - 'private.php' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K865.txt

vBulletin 3.0 - 'forumdisplay.php' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K822.txt

vBulletin 3.0 - 'search.php' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K691.txt

vBulletin 3.0 - 'showthread.php' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K8[01;31m[K23[m[K.txt
```

vBulletin 3.0.1 - 'newreply.php?WYSIWYG_HTML' Cross-Site Scripting
| php/webapps/24[01;31m[K23[m[K4.html

vBulletin vBSEO 4.x - 'visitormessage.php' Remote Code Injection
| php/webapps/36[01;31m[K23[m[K2.txt

VehicleWorkshop - SQL Injection
| php/webapps/4[01;31m[K23[m[K93.txt

VehicleWorkshop 1.0 - 'bookingid' SQL Injection
| php/webapps/480[01;31m[K23[m[K.txt

Ventrilo 3.0.2 - Null Pointer Remote Denial of Service
| multiple/dos/6[01;31m[K23[m[K7.txt

Vermillion FTP Daemon - 'PORT' Memory Corruption (Metasploit)
| windows/remote/167[01;31m[K23[m[K.rb

VeryPDF Image2PDF Converter - Local Buffer Overflow (SEH)
| windows/local/384[01;31m[K23[m[K.py

VICIdial 2.9 RC 1 < 2.13 RC1 - 'user_authorization' Command Execution
(Metasploit) |
unix/remote/4[01;31m[K23[m[K70.rb

VICIDIAL Call Center Suite 2.2.1-[01;31m[K23[m[K7 - Multiple
Vulnerabilities |
php/webapps/21220.txt

vicomsoft rapidcache server 2.0/2.2.6 - Directory Traversal
| windows/remote/[01;31m[K23[m[K544.txt

Vicomsoft RapidCache Server 2.0/2.2.6 - Host Argument Denial of Service
| multiple/dos/[01;31m[K23[m[K543.txt

Victory FTP Server 5.0 - Denial of Service
| windows/dos/16[01;31m[K23[m[K0.py

VideoCharge Studio 2.12.3.685 - Local Buffer Overflow (SEH)
| windows/local/29[01;31m[K23[m[K4.py

VideoGirls BiZ - Blind SQL Injection
| php/webapps/7[01;31m[K23[m[K4.txt

VideoLAN VLC Media Player 2.0.4 - '.swf' Crash (PoC)
| windows/dos/[01;31m[K23[m[K201.txt

VidiScript - SQL Injection
| php/webapps/162[01;31m[K23[m[K.txt

VieNuke VieBoard 2.6 - SQL Injection
| asp/webapps/[01;31m[K23[m[K335.txt

```
Vine VideoSite Creator Script - SQL Injection
| php/webapps/411[01;31m[K23[m[K.txt

ViRobot Linux Server 2.0 - Local Overflow
| linux/local/[01;31m[K23[m[K045.pl

Virtools Web Player 3.0.0.100 - Buffer Overflow (Denial of Service)
(PoC)                                  |
windows/dos/1[01;31m[K23[m[K9.c

Virtual Postage (VPA) - Man In The Middle Remote Code Execution
| android/remote/4[01;31m[K23[m[K50.txt

Virtual Programming VP-ASP 4.00/5.00 - 'shopdisplayproducts.asp' SQL
Injection                              |
asp/webapps/[01;31m[K23[m[K408.txt

Virtual Programming VP-ASP 4.00/5.00 - 'shopsearch.asp' SQL Injection
| asp/webapps/[01;31m[K23[m[K407.txt

Virtual Programming VP-ASP 4/5 - 'shopdisplayproducts.asp' Cross-Site
Scripting                              |
asp/webapps/[01;31m[K23[m[K415.txt

VirtuaSystems VirtuaNews 1.0.x (Multiple Modules) - Cross-Site
Scripting                                 |
php/webapps/[01;31m[K23[m[K792.txt

Viscom Image Viewer CP Pro 8.0/Gold 6.0 - ActiveX Control (Metasploit)
| windows/remote/181[01;31m[K23[m[K.rb

Viscom Software Movie Player Pro SDK ActiveX 6.8 - Remote Buffer
Overflow                                |
windows/remote/1[01;31m[K23[m[K20.txt

VisualShapers EZContents 1.4/2.0 - 'module.php' Remote Command
Execution                                  |
php/webapps/[01;31m[K23[m[K537.txt

VisualShapers EZContents 1.x/2.0 - 'archivednews.php' Arbitrary File
Inclusion                              |
php/webapps/[01;31m[K23[m[K684.txt

VisualShapers EZContents 1.x/2.0 - 'db.php' Arbitrary File Inclusion
| php/webapps/[01;31m[K23[m[K683.txt

Vitrax Pre-modded 1.0.6-r3 - Remote File Inclusion
| php/webapps/[01;31m[K23[m[K53.txt

Vivisimo Clustering Engine - Search Script Cross-Site Scripting
| java/webapps/[01;31m[K23[m[K268.txt
```

Vivvo Article Manager 3.2 - 'classified_path' File Inclusion
| php/webapps/[01;31m[K23[m[K39.txt

Vivvo Article Manager 3.2 - 'id' SQL Injection
| php/webapps/[01;31m[K23[m[K37.txt

Vixie Cron crontab 3.0 - Privilege Lowering Failure (2)
| linux/local/208[01;31m[K23[m[K.sh

Vizer Web Server 1.9.1 - Remote Denial of Service
| windows/dos/[01;31m[K23[m[K713.txt

VMWare Fusion - Local Privilege Escalation
| macos/local/48[01;31m[K23[m[K2.md

VMware Fusion 11.5.2 - Privilege Escalation
| macos/local/48[01;31m[K23[m[K5.sh

VMware Workstation for Linux 12.5.2 build-4638[01;31m[K23[m[K4 - ALSA Configuration Host Local Privilege Escalation | linux/local/42045.c

VocalTec VGW4/8 Telephony Gateway - Remote Authentication Bypass
| asp/webapps/[01;31m[K23[m[K813.txt

Vonage VDV-[01;31m[K23[m[K - Denial of Service
| hardware/dos/43164.py

Vonage VDV[01;31m[K23[m[K - Cross-Site Scripting
| hardware/webapps/43150.html

Vorbis Tools oggenc 1.4.0 - '.wav' Denial of Service
| linux/dos/4[01;31m[K23[m[K97.txt

Vpop3d - Remote Denial of Service
| windows/dos/[01;31m[K23[m[K053.pl

VPOPMail 0.9x - 'vpopmail.php' Remote Command Execution
| php/webapps/2[01;31m[K23[m[K43.txt

VS-Link-Partner 2.1 - 'script_pfad' Remote File Inclusion
| php/webapps/33[01;31m[K23[m[K.html

vTiger CRM 5.0.4 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K23[m[K07.txt

VxWorks 6.8 - TCP Urgent Pointer = 0 Integer Underflow
| vxworks/dos/47[01;31m[K23[m[K3.py

WapServ 1.0 - Denial of Service
| multiple/dos/[01;31m[K23[m[K051.txt

WarpSpeed 4nAlbum Module 0.92 - 'displaycategory.php?basepath' Remote File Inclusion | php/webapps/[01;31m[K23[m[K815.txt

WarpSpeed 4nAlbum Module 0.92 - 'modules.php?gid' SQL Injection | php/webapps/[01;31m[K23[m[K816.txt

WarpSpeed 4nAlbum Module 0.92 - 'nmimage.php?z' Cross-Site Scripting | php/webapps/[01;31m[K23[m[K817.txt

Warrior Kings 1.3 And Warrior Kings: Battles 1.[01;31m[K23[m[K - Remote Format String | multiple/remote/25691.txt

Warrior Kings: Battles 1.[01;31m[K23[m[K - Remote Denial of Service | multiple/dos/25692.txt

Watermark Master 2.2.[01;31m[K23[m[K - '.wstyle' Local Buffer Overflow (SEH) | windows/local/29594.py

Watermark Master 2.2.[01;31m[K23[m[K - Local Buffer Overflow (SEH) | windows/local/29327.py

Watson Management Console 4.11.2.G - Directory Traversal | hardware/webapps/[01;31m[K23[m[K995.txt

wb news (webmobo) 2.3.3 - Persistent Cross-Site Scripting | php/webapps/1[01;31m[K23[m[K[01;31m[K23[m[K.txt

WCMS 1.0b - Arbitrary Add Admin | php/webapps/65[01;31m[K23[m[K.py

WDTV Live SMP 2.03.20 - Remote Password Reset | hardware/webapps/4[01;31m[K23[m[K26.txt

Web Crossing Web Server 4.0/5.0 Component - Remote Denial of Service | windows/dos/[01;31m[K23[m[K648.pl

Web Server Creator 0.1 - 'l' Remote File Inclusion | php/webapps/[01;31m[K23[m[K18.txt

Web Wiz Forum 6.34/7.0/7.5 - Unauthorized Private Forum Access | asp/webapps/[01;31m[K23[m[K331.txt

WebCalendar 0.9.x (Multiple Modules) - SQL Injection | php/webapps/[01;31m[K23[m[K099.txt

Webcam Corp Webcam Watchdog 1.0/1.1/3.63 Web Server - Remote Buffer Overflow | windows/remote/[01;31m[K23[m[K514.pl

WebcamXP 3.72.440/4.05.280 Beta - '/pocketpc?camnum' Arbitrary Memory Disclosure |
multiple/webapps/31[01;31m[K23[m[K3.txt

WebcamXP 3.72.440/4.05.280 Beta - '/show_gallery_pic?id' Arbitrary Memory Disclosure |
multiple/webapps/31[01;31m[K23[m[K4.txt

Webchat 0.77 - 'Defines.php' Remote File Inclusion
| php/webapps/2[01;31m[K23[m[K18.txt

WebCortex WebStores2000 - 'error.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K23[m[K729.txt

WebCT Campus Edition 3.8/4.x - HTML Injection
| multiple/remote/[01;31m[K23[m[K893.txt

WebDAV Windows 10 - Remote Code Execution (RCE)
| windows/remote/5[01;31m[K23[m[K34.NA

WebDM CMS - SQL Injection
| php/webapps/141[01;31m[K23[m[K.txt

webessence 1.0.2 - Multiple Vulnerabilities
| php/webapps/1[01;31m[K23[m[K87.sh

Webfroot Shoutbox 2.32 - 'Viewshoutbox.php' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K474.txt

WebFS 1.x - 'Pathname' Buffer Overrun
| linux/remote/[01;31m[K23[m[K196.c

Webgate WebEye - Information Disclosure
| cgi/webapps/[01;31m[K23[m[K418.pl

webgrind 1.0 - 'file' Local File Inclusion
| php/webapps/185[01;31m[K23[m[K.txt

WeBid 1.0.6 - SQL Injection
| php/webapps/[01;31m[K23[m[K997.txt

WEBIGniter v28.7.[01;31m[K23[m[K - Stored Cross Site Scripting (XSS)
| php/webapps/51807.txt

WEBIGniter v28.7.[01;31m[K23[m[K - Stored XSS
| php/webapps/51900.txt

WEBIGniter v28.7.[01;31m[K23[m[K File Upload - Remote Code Execution
| php/webapps/51736.txt

WebKit - 'WebCore::AccessibilityNodeObject::textUnderElement' Use-After-Free |
multiple/dos/4[01;31m[K23[m[K60.html

WebKit -
'WebCore::AccessibilityRenderObject::handleAriaExpandedChanged' Use-
After-Free | multiple/dos/4[01;31m[K23[m[K61.html

WebKit - 'WebCore::getCachedWrapper' Use-After-Free
| multiple/dos/4[01;31m[K23[m[K67.html

WebKit - 'WebCore::InputType::element' Use-After-Free (1)
| multiple/dos/4[01;31m[K23[m[K64.html

WebKit - 'WebCore::Node::getFlag' Use-After-Free
| multiple/dos/4[01;31m[K23[m[K66.html

WebKit - 'WebCore::Node::nextSibling' Use-After-Free
| multiple/dos/4[01;31m[K23[m[K62.html

WebKit - 'WebCore::RenderObject' with Accessibility Enabled Use-After-
Free |
multiple/dos/4[01;31m[K23[m[K65.html

WebKit - 'WebCore::RenderSearchField::addSearchResult' Heap Buffer
Overflow |
multiple/dos/4[01;31m[K23[m[K63.html

WebKit - UXSS via XSLT and Nested Document Replacements
| multiple/dos/47[01;31m[K23[m[K7.txt

WebKit JSC - 'ArgumentsEliminationPhase::transform' Incorrect
LoadVarargs Handling |
multiple/dos/4[01;31m[K23[m[K76.html

WebKit JSC - 'arrayProtoFuncSplice' Uninitialized Memory Reference
| multiple/dos/4[01;31m[K23[m[K74.html

WebKit JSC - 'DFG::ByteCodeParser::flush(InlineStackEntry*
inlineStackEntry)' Incorrect Scope Register Han |
multiple/dos/4[01;31m[K23[m[K73.html

WebKit JSC - 'JSArray::appendMemcpy' Uninitialized Memory Copy
| multiple/dos/4[01;31m[K23[m[K75.html

WebKit JSC - 'JSObject::putInlineSlow' / 'JSValue::putToPrimitive'
Universal Cross-Site Scripting |
multiple/webapps/4[01;31m[K23[m[K78.html

WebKit JSC - 'ObjectPatternNode::appendEntry' Stack Use-After-Free
| multiple/dos/4[01;31m[K23[m[K77.txt

WebKitGTK 2.[01;31m[K23[m[K.90 / WebKitGTK+ 2.22.6 - Denial of Service
| linux/dos/46465.txt

WebMethods Integration Server 10.15.0.0000-0092 - Improper Access on Login Page | windows/remote/52[01;31m[K23[m[K7.txt

Webmin 1.920 - Unauthenticated Remote Code Execution (Metasploit) | linux/remote/47[01;31m[K23[m[K0.rb

WebRTC - H264 NAL Packet Processing Type Confusion | multiple/dos/451[01;31m[K23[m[K.txt

Websense Appliance Manager - Command Injection | java/webapps/364[01;31m[K23[m[K.txt

Websense Enterprise 4/5 - Blocked Sites Cross-Site Scripting | windows/remote/[01;31m[K23[m[K411.txt

Website Auction Marketplace 2.0.5 - 'cat_id' SQL Injection | php/webapps/43[01;31m[K23[m[K8.txt

WebsiteBaker Addon Concert Calendar 2.1.4 - Multiple Vulnerabilities | php/webapps/[01;31m[K23[m[K993.txt

webSPELL 4.01.01 - Database Backup Download | php/webapps/[01;31m[K23[m[K52.txt

WebStudio eCatalogue - Blind SQL Injection | php/webapps/72[01;31m[K23[m[K.txt

WebTrends Reporting Center 6.1 Management Interface - Full Path Disclosure | windows/remote/[01;31m[K23[m[K559.txt

WebWasher Classic 2.2/3.3 - Error Message Cross-Site Scripting | multiple/remote/[01;31m[K23[m[K380.txt

Wernhart Guestbook 2001.03.28 - Multiple SQL Injections | php/webapps/350[01;31m[K23[m[K.txt

Weyal CMS - Multiple SQL Injections | php/webapps/385[01;31m[K23[m[K.txt

WFChat 1.0 - Information Disclosure | multiple/remote/2[01;31m[K23[m[K88.txt

WFTPD Pro Server 3.[01;31m[K23[m[K.1.1 - 'APPE' Remote Buffer Overflow (PoC) | windows/dos/2734.py

WFTPD Server GUI 3.21 - Remote Denial of Service | windows/dos/[01;31m[K23[m[K842.pl

WGet 1.x - Insecure File Creation Race Condition | linux/local/241[01;31m[K23[m[K.sh

Whale Communications e-Gap Security Appliance 2.5 - Login Page Source Code Disclosure | hardware/remote/[01;31m[K23[m[K545.txt

WhatsUp Gold 16.3 - Remote Code Execution | asp/webapps/39[01;31m[K23[m[K1.py

WHMCompleteSolution (WHMCS) control (WHMCompleteSolution) - SQL Injection | php/webapps/1[01;31m[K23[m[K71.txt

WideChapter 3.0 - HTTP Request Buffer Overflow | multiple/dos/[01;31m[K23[m[K142.txt

WIDZ 1.0/1.5 - Remote Code Execution | linux/remote/[01;31m[K23[m[K054.txt

Wikepage Opus 13 2007.2 - 'index.php' Multiple Directory Traversal Vulnerabilities | php/webapps/316[01;31m[K23[m[K.txt

Wiki Web Help 0.2.7 - Cross-Site Scripting / HTML Injection | php/webapps/34[01;31m[K23[m[K5.txt

WikiWebHelp 0.3.3 - Cross-Site Request Forgery | php/webapps/15[01;31m[K23[m[K9.html

Winace UnAce 2.2 - Command Line Argument Buffer Overflow (1) | linux/remote/[01;31m[K23[m[K368.c

Winace UnAce 2.2 - Command Line Argument Buffer Overflow (2) | linux/remote/[01;31m[K23[m[K369.c

Winamp 5.34 - '.mp4' Code Execution | windows/local/38[01;31m[K23[m[K.c

WinComLPD Total 3.0.2.6[01;31m[K23[m[K - Remote Buffer Overflow / Authentication Bypass | multiple/remote/31106.txt

Windows 11 SMB Client - Privilege Escalation & Remote Code Execution (RCE) | windows/remote/5[01;31m[K23[m[K30.py

Windows 2024.15 - Unauthenticated Desktop Screenshot Capture | windows/remote/5[01;31m[K23[m[K00.py

Windows File Explorer Windows 10 Pro x64 - TAR Extraction | windows/remote/5[01;31m[K23[m[K25.py

Windows File Explorer Windows 11 ([01;31m[K23[m[KH2) - NTLM Hash Disclosure | windows/remote/5[01;31m[K23[m[K10.py

WINMOD 1.4 - '.lst' Local Stack Overflow
| windows/local/9[01;31m[K23[m[K4.pl

WinSyslog Interactive Syslog Server 4.21 - long Message Remote Denial of Service | windows/dos/[01;31m[K23[m[K242.pl

Wireless Drive 1.1.0 iOS - Multiple Web Vulnerabilities
| ios/webapps/3[01;31m[K23[m[K74.txt

Wireless Tools 26 (IWConfig) - ARGV Local Command Line Buffer Overflow (1) | linux/local/[01;31m[K23[m[K299.c

Wireless Tools 26 (IWConfig) - ARGV Local Command Line Buffer Overflow (2) | linux/local/[01;31m[K23[m[K300.c

Wireless Tools 26 (IWConfig) - ARGV Local Command Line Buffer Overflow (3) | linux/local/[01;31m[K23[m[K301.c

Wireshark - 'iseries_check_file_type' Stack Out-of-Bounds Read
| multiple/dos/393[01;31m[K23[m[K.txt

Wireshark - 'nettrace_3gpp_32_4[01;31m[K23[m[K_file_open' Stack Out-of-Bounds Read | multiple/dos/39326.txt

Wireshark 1.2.1 - TLS Dissector 1.2 Conversation Handling Remote Denial of Service | linux/dos/332[01;31m[K23[m[K.txt

Wireshark 2.2.6 - IPv6 Dissector Denial of Service
| multiple/dos/421[01;31m[K23[m[K.txt

Wireshark 2.4.0 < 2.4.2 / 2.2.0 < 2.2.10 - CIP Safety Dissector Crash
| multiple/dos/43[01;31m[K23[m[K3.txt

WM Downloader 3.0.0.9 - Local Buffer Overflow (Metasploit)
| windows/local/1[01;31m[K23[m[K88.rb

WM-News 0.5 - Multiple Remote File Inclusions
| php/webapps/[01;31m[K23[m[K26.txt

WMAPM 3.1 - Local Privilege Escalation
| linux/local/[01;31m[K23[m[K364.sh

Woltlab Burning Board 1.1.1/2.x - 'galerie_onfly.php' Cross-Site Scripting | php/webapps/273[01;31m[K23[m[K.txt

Woltlab Burning Board Regenbogenwiese 2007 Addon - SQL Injection
| php/webapps/290[01;31m[K23[m[K.txt

Wondershare Application Framework Service 2.4.3.[01;31m[K23[m[K1 - 'WsAppService' Unquote Service Path | windows/local/47617.txt

Wondershare Filmora 12.2.9.2[01;31m[K23[m[K3 - Unquoted Service Path | windows/local/51395.txt

Wordit Logbook 098b3 - Logbook.pl Remote Command Execution | cgi/webapps/2[01;31m[K23[m[K37.txt

WordPress Core 0.6/0.7 - 'Blog.header.php' SQL Injection | php/webapps/[01;31m[K23[m[K213.txt

WordPress Core 4.7.0/4.7.1 - Content Injection | linux/webapps/412[01;31m[K23[m[K.py

WordPress Digits Plugin 8.4.6.1 - Authentication Bypass via OTP Bruteforcing | multiple/webapps/5[01;31m[K23[m[K07.txt

WordPress File Upload Plugin < 4.[01;31m[K23[m[K.3 - Stored XSS | php/webapps/51899.txt

WordPress Plugin Ads Pro < 3.4 - Cross-Site Scripting / SQL Injection | php/webapps/4[01;31m[K23[m[K80.txt

WordPress Plugin Advanced Custom Fields - Remote File Inclusion (Metasploit) | php/remote/[01;31m[K23[m[K856.rb

WordPress Plugin Alert Before Your Post - 'name' Cross-Site Scripting | php/webapps/363[01;31m[K23[m[K.txt

WordPress Plugin Asset-Manager - Arbitrary '.PHP' File Upload (Metasploit) | php/remote/[01;31m[K23[m[K652.rb

WordPress Plugin bbPress - Multiple Vulnerabilities | php/webapps/2[01;31m[K23[m[K96.txt

WordPress Plugin Booking Calendar Contact Form 1.0.[01;31m[K23[m[K - Multiple Vulnerabilities | php/webapps/394[01;31m[K23[m[K.txt

WordPress Plugin Booking Calendar Contact Form 1.1.[01;31m[K23[m[K - Shortcode SQL Injection | php/webapps/39319.txt

WordPress Plugin Booking Calendar Contact Form 1.1.[01;31m[K23[m[K - SQL Injection | php/webapps/39309.txt

WordPress Plugin Calculated Fields Form 1.0.10 - SQL Injection
| php/webapps/36[01;31m[K23[m[K0.txt

WordPress Plugin Comment Rating 2.9.[01;31m[K23[m[K - Multiple
Vulnerabilities |
php/webapps/16221.txt

WordPress Plugin Easy Webinar - Blind SQL Injection
| php/webapps/2[01;31m[K23[m[K00.txt

WordPress Plugin Events Manager Extended - Persistent Cross-Site
Scripting |
php/webapps/149[01;31m[K23[m[K.txt

WordPress Plugin Forum Server 1.6.5 - SQL Injection
| php/webapps/16[01;31m[K23[m[K5.txt

WordPress Plugin foxypress 0.4.2.5 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K23[m[K74.txt

WordPress Plugin GigPress 2.1.10 - Persistent Cross-Site Scripting
| php/webapps/16[01;31m[K23[m[K2.txt

WordPress Plugin Google Document Embedder - Arbitrary File Disclosure
(Metasploit) |
php/webapps/[01;31m[K23[m[K970.rb

WordPress Plugin IBPS Online Exam 1.0 - SQL Injection / Cross-Site
Scripting |
php/webapps/4[01;31m[K23[m[K51.txt

WordPress Plugin IWantOneButton 3.0.1 - Multiple Vulnerabilities
| php/webapps/16[01;31m[K23[m[K6.txt

WordPress Plugin NextGEN Gallery 1.9.1 - 'photocrati_ajax' Arbitrary
File Upload |
php/webapps/39[01;31m[K23[m[K7.txt

WordPress Plugin Ninja Forms 3.3.13 - CSV Injection
| php/webapps/45[01;31m[K23[m[K4.txt

WordPress Plugin Photocart Link 1.6 - Local File Inclusion
| php/webapps/396[01;31m[K23[m[K.txt

Wordpress Plugin PicUploader 1.0 - Remote File Upload
| php/webapps/48[01;31m[K23[m[K8.txt

WordPress Plugin Pie Register 2.0.13 - Privilege Escalation
| php/webapps/358[01;31m[K23[m[K.txt

WordPress Plugin Popup Builder 3.69.6 - Multiple Stored Cross Site
Scripting |
php/webapps/49[01;31m[K23[m[K1.txt

```
WordPress Plugin Portable phpMyAdmin - Authentication Bypass
| php/webapps/[01;31m[K23[m[K356.txt

WordPress Plugin Pretty Link 1.4.56 - Multiple Cross-Site Scripting
Vulnerabilities                          |
php/webapps/36[01;31m[K23[m[K3.txt

WordPress Plugin Relevanssi 2.7.2 - Persistent Cross-Site Scripting
| php/webapps/16[01;31m[K23[m[K3.txt

WordPress Plugin Sabai Discuss - Cross-Site Scripting
| php/webapps/4[01;31m[K23[m[K17.txt

WordPress Plugin Security Audit 1.0.0 - Stored Cross Site Scripting
(XSS)                                    |
php/webapps/507[01;31m[K23[m[K.txt

WordPress Plugin Spider Event Calendar 1.3.0 - Multiple Vulnerabilities
| php/webapps/257[01;31m[K23[m[K.txt

WordPress Plugin Tagged Albums - 'id' SQL Injection
| php/webapps/380[01;31m[K23[m[K.txt

WordPress Plugin Ultimate Product Catalogue - SQL Injection (1)
| php/webapps/368[01;31m[K23[m[K.txt

WordPress Plugin UPM Polls 1.0.4 - Blind SQL Injection
| php/webapps/18[01;31m[K23[m[K1.txt

WordPress Plugin wp-people 2.0 - 'wp-people-popup.php' SQL Injection
| php/webapps/31[01;31m[K23[m[K0.txt

WordPress Plugin WP-Property - Arbitrary '.PHP' File Upload
(Metasploit)                                  |
php/remote/[01;31m[K23[m[K651.rb

WordPress Plugin WPsc MijnPress - 'rwflush' Cross-Site Scripting
| php/webapps/371[01;31m[K23[m[K.txt

WordPress Plugin wpStoreCart 2.5.27-2.5.29 - Arbitrary File Upload
| php/webapps/190[01;31m[K23[m[K.php

WordPress Plugin WPtouch 1.9.27 - URL redirection
| php/webapps/174[01;31m[K23[m[K.txt

WordPress Theme Chocolate WP - Multiple Vulnerabilities
| php/webapps/38[01;31m[K23[m[K7.txt

WordPress Theme Clockstone (and other CMSMasters Themes) - Arbitrary
File Upload                              |
php/webapps/[01;31m[K23[m[K494.txt
```

```
WordPress User Registration & Membership Plugin 4.1.2 - Authentication
Bypass                                  |
multiple/webapps/5[01;31m[K23[m[K02.py

WorkgroupMail 7.5.1 - 'WorkgroupMail' Unquoted Service Path
| windows/local/475[01;31m[K23[m[K.txt

Working Resources BadBlue Server 2.40 - 'PHPtest.php' Full Path
Disclosure                                      |
php/webapps/[01;31m[K23[m[K753.txt

WrenSoft Zoom Search Engine 2.0 Build: 1018 - Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K244.txt

WSMP3 0.0.x - Remote Command Execution
| linux/remote/226[01;31m[K23[m[K.txt

WSN Guest 1.[01;31m[K23[m[K - 'Search' SQL Injection
| php/webapps/7659.txt

WSN Links 2.22/2.[01;31m[K23[m[K - 'vote.php' SQL Injection
| php/webapps/6524.txt

WSO2 Identity Server 5.1.0 - Multiple Vulnerabilities
| jsp/webapps/40[01;31m[K23[m[K9.txt

WTools 0.0.1a - 'INCLUDE_PATH' Remote File Inclusion
| php/webapps/[01;31m[K23[m[K46.txt

WU-FTPD 2.6.0 - Remote Format Strings
| solaris/remote/[01;31m[K23[m[K9.c

WzdFTPD 0.1 rc5 - Login Remote Denial of Service
| windows/dos/[01;31m[K23[m[K169.pl

WzdFTPD 0.5.4 - Remote Command Execution
| linux/remote/1[01;31m[K23[m[K1.pl

X-Chat 2.0.6 - Remote Denial of Service
| linux/dos/[01;31m[K23[m[K438.pl

X-Skipper-Proxy v0.13.[01;31m[K23[m[K7 - Server Side Request Forgery
(SSRF)                                                  |
multiple/remote/51111.txt

X11R6 < 6.4 XKEYBOARD (sco x86) - Local Buffer Overflow
| sco/local/[01;31m[K23[m[K32.c

X11R6 < 6.4 XKEYBOARD (solaris x86) - Local Buffer Overflow
| solaris/local/[01;31m[K23[m[K31.c

X11R6 < 6.4 XKEYBOARD (Solaris/SPARC) - Local Buffer Overflow (1)
| solaris/local/[01;31m[K23[m[K30.c
```

X11R6 < 6.4 XKEYBOARD (Solaris/SPARC) - Local Buffer Overflow (2)
| solaris/local/[01;31m[K23[m[K60.c

X2Engine 4.2 - Arbitrary File Upload
| php/webapps/383[01;31m[K23[m[K.txt

X7 Chat 2.0.5 - Authentication Bypass
| php/webapps/71[01;31m[K23[m[K.txt

xClassified - 'ads.php' SQL Injection
| php/webapps/39[01;31m[K23[m[K9.txt

Xenon - 'id' Multiple SQL Injections
| php/webapps/36[01;31m[K23[m[K6.txt

Xerox MicroServer - Web Server Directory Traversal
| unix/remote/[01;31m[K23[m[K449.txt

XFree86 4.2 - 'XLOCALEDIR' Local Buffer Overflow (1)
| linux/local/2[01;31m[K23[m[K20.c

XFree86 4.2 - 'XLOCALEDIR' Local Buffer Overflow (2)
| linux/local/2[01;31m[K23[m[K21.c

XFree86 4.2 - 'XLOCALEDIR' Local Buffer Overflow (3)
| linux/local/2[01;31m[K23[m[K22.c

XFree86 4.2 - 'XLOCALEDIR' Local Buffer Overflow (4)
| linux/local/2[01;31m[K23[m[K[01;31m[K23[m[K.c

XFree86 4.3 - Font Information File Buffer Overflow
| linux/local/[01;31m[K23[m[K682.c

XFree86 4.x - CopyISOLatin1Lowered Font_Name Buffer Overflow
| linux/dos/[01;31m[K23[m[K690.txt

XFTP 3.0 Build 0[01;31m[K23[m[K9 - 'Filename' Remote Buffer Overflow
| windows/remote/12834.py

Xftp client 3.0 - 'PWD' Remote Overflow
| windows/remote/1[01;31m[K23[m[K32.pl

Ximian Evolution 1.x - MIME image/* Content-Type Data Inclusion
| linux/remote/2[01;31m[K23[m[K71.txt

Ximian Evolution 1.x - UUEncoding Denial of Service
| linux/dos/2[01;31m[K23[m[K70.txt

Ximian Evolution 1.x - UUEncoding Parsing Memory Corruption
| linux/remote/2[01;31m[K23[m[K69.txt

Xlight FTP Server 1.25/1.41 - 'PASS' Remote Buffer Overflow
| windows/dos/[01;31m[K23[m[K468.pl

Xlight FTP Server 1.52 - Remote Send File Request Denial of Service
| windows/dos/[01;31m[K23[m[K701.txt

Xlight FTP Server 1.x - Long Directory Request Remote Denial of Service
| windows/dos/[01;31m[K23[m[K654.txt

XMB Forum 1.8 - 'editprofile.php?user' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K746.txt

XMB Forum 1.8 - 'forumdisplay.php' Multiple SQL Injections
| php/webapps/[01;31m[K23[m[K748.txt

XMB Forum 1.8 - 'u2uadmin.php?uid' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K745.txt

XMB Forum 1.8 - BBcode align Tag Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K747.txt

Xoops 1.0/1.3.x - BBCode HTML Injection
| php/webapps/[01;31m[K23[m[K026.txt

Xoops 1.3.x/2.0.x - Multiple Vulnerabilities
| php/webapps/[01;31m[K23[m[K416.txt

XOOPS 2.0 XoopsOption - Information Disclosure
| php/webapps/2[01;31m[K23[m[K89.txt

Xoops 2.0.5.1 - 'MyLinks Myheader.php' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K459.txt

Xoops 2.0.x - 'viewtopic.php' Cross-Site Scripting
| php/webapps/[01;31m[K23[m[K606.txt

Xoops 2.5.4 - Blind SQL Injection
| php/webapps/18[01;31m[K23[m[K3.txt

XOOPS Module eCal 2.24 - 'display.php' SQL Injection
| php/webapps/36[01;31m[K23[m[K.pl

Xplico 0.5.7 - 'add.ctp' Cross-Site Scripting (2)
| multiple/webapps/34[01;31m[K23[m[K7.txt

XRms 1.99.2 - 'campaign_title' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K[01;31m[K23[m[K.txt

XRms 1.99.2 - 'case_title' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K25.txt

XRms 1.99.2 - 'company_name' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K21.txt

XRms 1.99.2 - 'file_id' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K26.txt

XRms 1.99.2 - 'last_name' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K22.txt

XRms 1.99.2 - 'login.php?target' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K18.txt

XRms 1.99.2 - 'opportunity_title' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K24.txt

XRms 1.99.2 - 'starting' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K27.txt

XRms 1.99.2 - 'title' Cross-Site Scripting
| php/webapps/3[01;31m[K23[m[K20.txt

XSOK 1.0 2 - 'LANG Environment' Local Buffer Overrun
| linux/local/[01;31m[K23[m[K510.c

XtremeASP PhotoGallery 2.0 - 'Adminlogin.asp' SQL Injection
| asp/webapps/[01;31m[K23[m[K547.txt

xweb 1.0 - Directory Traversal
| linux/remote/[01;31m[K23[m[K864.txt

YABB SE 1.5 - 'Quote' SQL Injection
| php/webapps/[01;31m[K23[m[K710.txt

YABB SE 1.5.1 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K23[m[K812.txt

YaBB SE 1.5.x - Arbitrary File Deletion
| php/webapps/[01;31m[K23[m[K774.txt

YaBB SE 1.5.x - Multiple SQL Injections
| php/webapps/[01;31m[K23[m[K775.txt

YABB SE 1.x - 'SSI.php' ID_MEMBER SQL Injection
| php/webapps/[01;31m[K23[m[K554.java

Yahoo! Messenger 4.0/5.0 - Remote Denial of Service
| windows/dos/[01;31m[K23[m[K086.txt

Yahoo! Messenger 5.6 - File Transfer Buffer Overrun
| windows/dos/[01;31m[K23[m[K293.txt

Yahoo! Webcam ActiveX Control 2.0.0.107 - Buffer Overrun
| windows/remote/[01;31m[K23[m[K152.txt

YaSoft Switch Off 2.3 - 'swnet.dll' Remote Buffer Overflow
| windows/remote/[01;31m[K23[m[K509.c

YaSoft Switch Off 2.3 - Large Packet Remote Denial of Service
| hardware/dos/[01;31m[K23[m[K508.txt

Yaws 1.91 - Remote File Disclosure
| multiple/remote/4[01;31m[K23[m[K03.txt

YeaLink IP Phone SIP-TxxP Firmware 9.70.0.100 - Multiple
Vulnerabilities |
hardware/webapps/[01;31m[K23[m[K572.txt

Yelp 2.[01;31m[K23[m[K.1 - Invalid URI Format String
| linux/dos/32248.txt

yMonda Thread-IT 1.6 - Multiple HTML Injections
| php/webapps/[01;31m[K23[m[K175.txt

Yoxel 1.[01;31m[K23[m[Kbeta - 'itpm_estimate.php' Remote Code Execution
| php/webapps/6606.txt

Yukihiro Matsumoto Ruby 1.x - XMLRPC Server Denial of Service
| linux/dos/277[01;31m[K23[m[K.txt

Zabbix 2.2.x/3.0.x - SQL Injection
| php/webapps/40[01;31m[K23[m[K7.txt

Zabbix 7.0.0 - SQL Injection
| php/webapps/52[01;31m[K23[m[K0.py

ZaireWeb Solutions NewsLetter ZWS - Administrative Interface
Authentication Bypass |
php/webapps/24[01;31m[K23[m[K5.txt

Zanfi CMS lite / Jaw Portal free - 'page' SQL Injection
| php/webapps/64[01;31m[K23[m[K.txt

zawhttpd 0.8.[01;31m[K23[m[K - GET Remote Buffer Overflow (Denial of
Service) (PoC) | linux/dos/1746.pl

Zechat 1.5 - 'uname' SQL Injection
| php/webapps/455[01;31m[K23[m[K.txt

ZeeBuddy 2.1 - 'adid' SQL Injection
| php/webapps/6[01;31m[K23[m[K0.txt

ZenPhoto 1.1.3 - 'rss.php?albumnr' SQL Injection
| php/webapps/48[01;31m[K23[m[K.pl

ZeroShell 1.0beta11 - Remote Code Execution
| hardware/remote/80[01;31m[K23[m[K.txt

ZesleCP 3.1.9 - Remote Code Execution (RCE) (Authenticated)
| multiple/webapps/50[01;31m[K23[m[K3.py

ZeusCart - 'prodid' SQL Injection
| php/webapps/392[01;31m[K23[m[K.txt

ZeusCart 4.0 - Cross-Site Request Forgery
| php/webapps/382[01;31m[K23[m[K.txt

zFTPServer Suite 6.0.0.52 - 'rmdir' Directory Traversal
| windows/remote/18[01;31m[K23[m[K5.pl

Zillya Total Security 3.0.[01;31m[K23[m[K67.0 - Local Privilege
Escalation |
windows/local/51151.txt

ZipGenius 6.3.1.2552 - 'zgtips.dll' Local Stack Buffer Overflow
| windows/local/1[01;31m[K23[m[K26.py

ZipWrangler 1.20 - '.zip' File (SEH)
| windows/local/1[01;31m[K23[m[K68.pl

Zix Forum 1.12 - 'RepId' SQL Injection (1)
| asp/webapps/[01;31m[K23[m[K06.txt

Zix Forum 1.12 - 'RepId' SQL Injection (2)
| php/webapps/[01;31m[K23[m[K82.pl

ZKTeco ZKAccess Professional 3.5.3 - Insecure File Permissions
Privilege Escalation |
windows/local/403[01;31m[K23[m[K.txt

ZOC Terminal 7.[01;31m[K23[m[K.4 - 'Script' Denial of Service (PoC)
| windows/dos/46855.py

ZOC Terminal v7.[01;31m[K23[m[K.4 - 'Private key file' Denial of
Service (PoC) |
windows/dos/46856.py

ZOC Terminal v7.[01;31m[K23[m[K.4 - 'Shell' Denial of Service (PoC)
| windows/dos/46857.py

ZoneAlarm 3.7.202/PRO 4.0/PRO 4.5 - Random UDP Flood Denial of Service
(1) | windows/dos/[01;31m[K23[m[K088.pl

ZoneAlarm 3.7.202/PRO 4.0/PRO 4.5 - Random UDP Flood Denial of Service
(2) | windows/dos/[01;31m[K23[m[K089.c

ZoneAlarm 3.7.202/PRO 4.0/PRO 4.5 - Random UDP Flood Denial of Service
(3) |
windows/dos/[01;31m[K23[m[K090.asm

ZoneAlarm Security Suite 7.0 - AntiVirus Directory Path Buffer Overflow
(PoC) | windows/dos/3[01;31m[K23[m[K56.txt

Zoneminder 1.29/1.30 - Cross-Site Scripting / SQL Injection / Session
Fixation / Cross-Site Request Forger |
php/webapps/41[01;31m[K23[m[K9.txt

```
Zoom Meeting Connector 4.6.[01;31m[K23[m[K9.20200613 - Remote Root
Exploit (Authenticated)                                  |
linux/webapps/49360.py

Zortam MP3 Media Studio [01;31m[K23[m[K.45 - Local Buffer Overflow
(SEH)                                                    |
windows/dos/44468.py

Zortam MP3 Media Studio [01;31m[K23[m[K.95 - Denial of Service (PoC)
| windows_x86-64/dos/45222.py

ZTE ZXV10 W300 v3.1.0c_DR0 - UI Session Delete
| hardware/webapps/373[01;31m[K23[m[K.txt

ZyXEL VMG3312-B10B - Cross-Site Scripting
| hardware/webapps/45[01;31m[K23[m[K6.txt

ZYXEL ZyWALL 10 Management Interface - Cross-Site Scripting
| hardware/remote/[01;31m[K23[m[K527.txt

---------------------------------------------------------------------------------------- ----------------
----------

---------------------------------------------------------------------------------------- ----------------
----------
Shellcode Title
|  Path

---------------------------------------------------------------------------------------- ----------------
----------
Apple macOS - Bind (4444/TCP) Shell (/bin/sh) + Null-Free Shellcode
(1[01;31m[K23[m[K bytes)                                 | macos/46396.c

FreeBSD/x86 - execv(/bin/sh) Shellcode ([01;31m[K23[m[K bytes)
| freebsd_x86/43504.asm

FreeBSD/x86 - execve(/bin/sh) Shellcode ([01;31m[K23[m[K bytes) (1)
| freebsd_x86/13272.c

FreeBSD/x86 - execve(/bin/sh) Shellcode ([01;31m[K23[m[K bytes) (2)
| freebsd_x86/13273.c

Linux/ARM - Bind (1[01;31m[K23[m[K4/TCP) Shell (/bin/sh) Shellcode (104
bytes)                                                   | arm/45029.c

Linux/SPARC - Reverse (192.168.100.1:[01;31m[K23[m[K13/TCP) Shell
Shellcode (216 bytes)                                    |
linux_sparc/13305.c

Linux/Tru64 alpha - execve(/bin/sh) Shellcode (108 bytes)
| linux/47[01;31m[K23[m[K9.c
```

Linux/x64 - Bind (31173/TCP) Shell (/bin/sh) + Password (1[01;31m[K23[m[K4) Shellcode (92 bytes) | linux_x86-64/38469.c

Linux/x64 - Bind (4444/TCP) Shell (/bin/sh) + Password (1[01;31m[K23[m[K4567) Shellcode (136 bytes) | linux_x86-64/43951.nasm

Linux/x64 - Bind_tcp (0.0.0.0:4444) + Password (1[01;31m[K23[m[K45678) + Shell (/bin/sh) Shellcode (142 bytes) | linux/49472.c

Linux/x64 - execve() Shellcode (22 bytes) | linux_x86-64/38[01;31m[K23[m[K9.asm

Linux/x64 - execve(/bin/sh) Shellcode ([01;31m[K23[m[K bytes) | linux_x86-64/46907.c

Linux/x64 - execve(/bin/sh) Via Push Shellcode ([01;31m[K23[m[K bytes) | linux_x86-64/36858.c

Linux/x64 - Fork Bomb Shellcode (11 bytes) | linux_x86-64/425[01;31m[K23[m[K.c

Linux/x64 - Reverse (127.0.0.1:4444/TCP) Shell (/bin/sh) + Password (1[01;31m[K23[m[K4567) Shellcode (104 bytes) | linux_x86-64/43952.nasm

Linux/x64 - Reverse (192.168.1.2:1[01;31m[K23[m[K4/TCP) Shell Shellcode (134 bytes) | linux_x86-64/39578.c

Linux/x64 - Reverse (192.168.1.8:4444/TCP) Shell Shellcode (104 bytes) | linux_x86-64/4[01;31m[K23[m[K39.c

Linux/x64 - Reverse Netcat Shell (127.0.0.1:1[01;31m[K23[m[K4) + Polymorphic Shellcode (106 bytes) | linux_x86-64/41510.nsam

Linux/x86 - Bind (1[01;31m[K23[m[K4/TCP) Shell (/bin/sh) Shellcode (87 bytes) (Generator) | generator/39815.c

Linux/x86 - Bind (1472/TCP) Shell (/bin/sh) + IPv6 Shellcode (1250 bytes) | linux_x86/397[01;31m[K23[m[K.c

Linux/x86 - Bind (31337/TCP) Netcat Shell + Polymorphic Shellcode (91 bytes) | linux_x86/14[01;31m[K23[m[K5.c

Linux/x86 - Bind (4444/TCP) Shell (/bin/sh) + IPv6 Shellcode (113 bytes) | linux_x86/447[01;31m[K23[m[K.c

Linux/x86 - Bind (6778/TCP) Shell + Polymorphic + XOR Encoded Shellcode (125 bytes) | linux_x86/14[01;31m[K23[m[K4.c

Linux/x86 - chmod 0777 /etc/shadow + sys_chmod syscall Shellcode (39 bytes) | linux_x86/137[01;31m[K23[m[K.c

Linux/x86 - Disable ASLR Security + Obfuscated Shellcode ([01;31m[K23[m[K bytes) | linux_x86/43897.nasm

Linux/x86 - execve() Shellcode ([01;31m[K23[m[K bytes) | linux_x86/13422.c

Linux/x86 - execve(/bin/sh) + PUSH Shellcode ([01;31m[K23[m[K bytes) | linux_x86/13399.c

Linux/x86 - execve(/bin/sh) + sysenter Opcode Array Payload Shellcode ([01;31m[K23[m[K bytes) | linux_x86/13412.c

Linux/x86 - execve(/bin/sh) Shellcode ([01;31m[K23[m[K bytes) (1) | linux_x86/37384.c

Linux/x86 - execve(/bin/sh) Shellcode ([01;31m[K23[m[K bytes) (2) | linux_x86/43722.c

Linux/x86 - execve(_/bin/ash__0_0) Shellcode (21 bytes) | linux_x86/134[01;31m[K23[m[K.c

Linux/x86 - execve(_/bin/sh__ [_/bin/sh__ NULL]) Shellcode ([01;31m[K23[m[K bytes) | linux_x86/13376.c

Linux/x86 - Perl Script Execution Shellcode (99+ bytes) | linux_x86/133[01;31m[K23[m[K.c

Linux/x86 - Random Insertion Encoder and Decoder Shellcode (Generator) | linux_x86/463[01;31m[K23[m[K.py

Linux/x86 - Raw-Socket ICMP/Checksum Shell (/bin/sh) Shellcode ([01;31m[K23[m[K5 bytes) | linux_x86/13343.asm

Linux/x86 - read(0_buf_2541) + chmod(buf_4755) Shellcode ([01;31m[K23[m[K bytes) | linux_x86/13406.c

Linux/x86 - Remote Port Forwarding (ssh -R 9999:localhost:22 192.168.0.226) Shellcode (87 bytes) | linux_x86/[01;31m[K23[m[K622.c

Linux/x86 - Reverse (127.1.1.1:1[01;31m[K23[m[K45/TCP) cat /etc/passwd Shellcode (111 bytes) | linux_x86/43747.c

Linux/x86 - Reverse (127.255.255.254:9090/TCP) Shell (/bin/zsh) Shellcode (80 bytes) | linux_x86/402[01;31m[K23[m[K.c

```
Linux/x86 - Reverse (192.168.3.119:54321/TCP) Shell (/bin/bash)
Shellcode (110 bytes)                       |
linux_x86/417[01;31m[K23[m[K.c

Linux/x86 - Reverse (200.182.207.[01;31m[K23[m[K5/TCP) Telnet Shel
Shellcode (134 bytes)                                |
linux_x86/13435.c

Linux/x86 - Reverse
(fd15:4ba5:5a2b:1002:61b7:[01;31m[K23[m[Ka9:ad3d:5509:1337/TCP) Shell
(/bin/sh) + IPv6 Shellcode (G | linux_x86/45292.py

Linux/x86 - TCP Proxy (192.168.1.16:1280/TCP) All Connect() + Null-Free
Shellcode ([01;31m[K23[m[K6 bytes)              | linux_x86/13381.c

Mainframe/System Z - Bind (1[01;31m[K23[m[K45/TCP) Shell + Null-Free
Shellcode (2488 bytes)                             | system_z/38075.txt

NetBSD/x86 - Kill All Processes Shellcode ([01;31m[K23[m[K bytes)
| netbsd_x86/13470.c

OpenBSD/x86 - execve(/bin/sh) Shellcode ([01;31m[K23[m[K bytes)
| openbsd_x86/13475.c

Solaris/SPARC - Bind (/TCP) Shell Shellcode
| solaris_sparc/436[01;31m[K23[m[K.asm

Windows (NT/2000/XP) (Russian) - Add Administartor User (slim/shady)
Shellcode (318 bytes)                 |
windows_x86/135[01;31m[K23[m[K.c

Windows - Add Administrator User (RubberDuck/mudbath) + ExitProcess
WinExec Shellcode (279 bytes)          | windows/173[01;31m[K23[m[K.c

Windows - MessageBoxA() Shellcode ([01;31m[K23[m[K8 bytes)
| windows/13828.c

Windows - Reverse (127.0.0.1:1[01;31m[K23[m[K/TCP) Shell + Alphanumeric
Shellcode (Encoder/Decoder) (Generator)         | generator/13286.c

Windows/x64 - Dynamic MessageBoxA or MessageBoxW PEB & Import Table
Method Shellcode ([01;31m[K23[m[K2 bytes)           | windows_x86-
64/48229.txt

Windows/x64 - Reverse (192.168.[01;31m[K23[m[K2.129:4444/TCP) Shell +
Injection Shellcode (694 bytes)                   | windows_x86-
64/40781.c

Windows/x86 (PerfectXp-pc1/SP3 ) (Turkish) - Add Administrator User
(kpss/1[01;31m[K23[m[K45) Shellcode (112 bytes)     |
windows_x86/17545.c
```

Windows/x86 (XP Pro SP3) - Download File Via TFTP + Execute Shellcode (51-60 bytes) (Generator) | generator/461[01;31m[K23[m[K.py

Windows/x86 (XP SP2) (English / Arabic) - cmd.exe Shellcode ([01;31m[K23[m[K bytes) | windows_x86/13574.c

Windows/x86 (XP SP2) (English) - cmd.exe Shellcode ([01;31m[K23[m[K bytes) | windows_x86/13505.c

Windows/x86 (XP SP3) (Turkish) - Add Administrator User (zrl/1[01;31m[K23[m[K456) Shellcode (127 bytes) | windows_x86/15063.c

Windows/x86 - Add Administrator User (GAZZA/1[01;31m[K23[m[K456) + Start Telnet Service Shellcode (111 bytes) | windows_x86/13508.asm

Windows/x86 - MessageBoxA PEB & Export Address Table NullFree/Dynamic Shellcode ([01;31m[K23[m[K0 bytes) | windows_x86/50369.c

Windows/x86 - Reverse (192.168.[01;31m[K23[m[K2.129:4444/TCP) Shell + Persistent Access Shellcode (494 bytes) | windows_x86/40334.c

---

Port: 25

Exploit Title | Path

(Bitcoin / Dogecoin) PHP Cloud Mining Script - Authentication Bypass | php/webapps/4[01;31m[K25[m[K31.txt

10-Strike Network Inventory Explorer - 'srvInventoryWebServer' Unquoted Service Path | windows/local/48[01;31m[K25[m[K1.txt

10-Strike Network Inventory Explorer 8.54 - 'Add' Local Buffer Overflow (SEH) | windows/local/48[01;31m[K25[m[K3.py

12Planet Chat Server 2.9 - Cross-Site Scripting | multiple/remote/24[01;31m[K25[m[K3.txt

```
24online SMS_[01;31m[K25[m[K00i 8.3.6 build 9.0 - SQL Injection
| jsp/webapps/40060.txt

[01;31m[K25[m[K32/Gigs 1.2.1 - 'activateuser.php' Local File Inclusion
| php/webapps/4317.txt

[01;31m[K25[m[K32/Gigs 1.2.2 - Arbitrary Database Backup/Download
| php/webapps/5465.txt

[01;31m[K25[m[K32/Gigs 1.2.2 Stable - Multiple Vulnerabilities
| php/webapps/7510.txt

[01;31m[K25[m[K32/Gigs 1.2.2 Stable - Remote Authentication Bypass
| php/webapps/7511.txt

[01;31m[K25[m[K32/Gigs 1.2.2 Stable - Remote Command Execution
| php/webapps/7512.php

29o3 CMS - 'LibDir' Multiple Remote File Inclusions
| php/webapps/1[01;31m[K25[m[K58.txt

2BGal 2.5.1 - SQL Injection
| php/webapps/[01;31m[K25[m[K045.txt

2DayBiz Job Site Script - SQL Injection
| php/webapps/140[01;31m[K25[m[K.txt

2X ApplicationServer 10.1 - TuxSystem Class ActiveX Control Remote File
Overwrite                           |
windows/remote/186[01;31m[K25[m[K.txt

3Com FTP Server 2.0 - Remote Overflow
| windows/remote/8[01;31m[K25[m[K.c

3Com Wireless 8760 Dual-Radio 11a/b/g PoE - Multiple Vulnerabilities
| hardware/remote/3[01;31m[K25[m[K91.txt

3D-FTP Client 4.0 - Buffer Overflow
| windows/dos/2[01;31m[K25[m[K51.pl

4 TOTOLINK Router Models - Backdoor Credentials
| hardware/webapps/376[01;31m[K25[m[K.txt

427BB 2.x - Multiple Remote HTML Injection Vulnerabilities
| php/webapps/[01;31m[K25[m[K178.txt

4D WebSTAR 5.3/5.4 Tomcat Plugin - Remote Buffer Overflow
| osx/remote/[01;31m[K25[m[K626.c

4Images 1.7.7 - 'image_utils.php' Remote Command Execution
| php/webapps/1[01;31m[K25[m[K85.txt
```

68KB Knowledge Base Script 1.0.0rc2 - Search SQL Injection
| php/webapps/119[01;31m[K25[m[K.txt

724CMS Enterprise 4.59 - 'section.php' Local File Inclusion
| php/webapps/1[01;31m[K25[m[K65.txt

724CMS Enterprise 4.59 - 'section.php' SQL Injection
| php/webapps/1[01;31m[K25[m[K66.txt

724CMS Enterprise 4.59 - SQL Injection
| php/webapps/1[01;31m[K25[m[K60.txt

ABB Cylon Aspect 3.08.02 (deployStart.php) - Unauthenticated Command
Execution |
php/hardware/52[01;31m[K25[m[K1.txt

ABB Cylon Aspect 3.08.02 (ethernetUpdate.php) - Authenticated Path
Traversal |
php/hardware/52[01;31m[K25[m[K2.txt

ABBS Audio Media Player 3.1 - '.lst' Local Buffer Overflow
| windows/local/[01;31m[K25[m[K204.py

ABC2MIDI 2004-12-04 - Multiple Stack Buffer Overflow Vulnerabilities
| multiple/remote/[01;31m[K25[m[K019.txt

ABC2MTEX 1.6.1 - Command Line Stack Overflow
| linux/dos/47[01;31m[K25[m[K4.txt

ABC2MTEX 1.6.1 - Process ABC Key Field Buffer Overflow
| multiple/remote/[01;31m[K25[m[K018.txt

ABC2PS/JCABC2PS 1.2 - Voice Field Buffer Overflow
| windows/remote/[01;31m[K25[m[K0[01;31m[K25[m[K.txt

ABCPP 1.3 - Directive Handler Buffer Overflow
| windows/remote/[01;31m[K25[m[K021.txt

abctab2ps 1.6.3 - 'Trim_Title' '.ABC' File Remote Buffer Overflow
| windows/remote/[01;31m[K25[m[K029.txt

abctab2ps 1.6.3 - 'Write_Heading' '.ABC' Remote Buffer Overflow
| windows/remote/[01;31m[K25[m[K027.txt

ac4p Mobile - 'up.php?Taaa' Cross-Site Scripting
| php/webapps/292[01;31m[K25[m[K.txt

Achat 0.150 beta7 - Remote Buffer Overflow
| windows/remote/360[01;31m[K25[m[K.py

Achievo 1.4.5 - Multiple Vulnerabilities (2)
| php/webapps/23[01;31m[K25[m[K3.txt

ACNews 1.0 - Authentication Bypass
| asp/webapps/9[01;31m[K25[m[K.txt

Acoustica Audio Converter Pro 1.1 (build [01;31m[K25[m[K) - '.mp3 / .wav / .ogg / .wma' Local Heap Overflow | windows/local/15069.py

ACS Blog 0.8/0.9/1.0/1.1 - 'Name' HTML Injection
| asp/webapps/[01;31m[K25[m[K313.txt

ACS Blog 0.8/0.9/1.0/1.1 - 'search.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K233.txt

ActFax Server (LPD/LPR) 4.[01;31m[K25[m[K Build 0221 (2010-02-11) - Remote Buffer Overflow | windows/remote/16176.pl

ActFax Server 4.31 Build 02[01;31m[K25[m[K - Local Privilege Escalation
| windows/local/20915.py

ActFax Server FTP 4.[01;31m[K25[m[K Build 0221 (2010-02-11) - (Authenticated) Remote Buffer Overflow | windows/remote/16177.py

Active Auction House - 'account.asp?ReturnURL' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K349.txt

Active Auction House - 'default.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K346.txt

Active Auction House - 'ItemInfo.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K347.txt

Active Auction House - 'sendpassword.asp' Multiple Cross-Site Scripting Vulnerabilities | asp/webapps/[01;31m[K25[m[K351.txt

Active Auction House - 'start.asp?ReturnURL' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K348.txt

Active Auction House - 'WatchThisItem.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K352.txt

Active Bulletin Board 1.1b2 - Remote User Pass Change
| asp/webapps/[01;31m[K25[m[K92.html

Active News Manager - 'login.asp' SQL Injection
| solaris/local/[01;31m[K25[m[K703.txt

ActivePDF Toolkit < 8.1.0.19023 - Multiple Memory Corruptions
| windows/dos/44[01;31m[K25[m[K1.txt

ActiveWeb Professional 3.0 - Arbitrary File Upload
| cfm/webapps/35[01;31m[K25[m[K6.txt

Adam Wright HTMLTidy 0.5 - 'html-tidy-logic.php' Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K27.txt

Administrador de Contenidos - Admin Authentication Bypass
| asp/dos/1[01;31m[K25[m[K27.txt

Adobe Acrobat 7.0 / Adobe Reader 7.0 - File Existence / File Disclosure
| windows/remote/[01;31m[K25[m[K822.xml

Adobe Acrobat CoolType (AFDKO) - Memory Corruption in the Handling of
Type 1 Font load/store Operators |
windows/dos/47[01;31m[K25[m[K9.txt

Adobe Flash - Out-of-Bounds Read when Placing Object
| multiple/dos/398[01;31m[K25[m[K.txt

Adobe Shockwave Player 11.5.6.606 - 'DIR' Multiple Memory
Vulnerabilities |
windows/dos/1[01;31m[K25[m[K78.c

Adobe SVG Viewer 3.0 - ActiveX Control SRC Information Disclosure
| windows/remote/[01;31m[K25[m[K597.txt

AdobeCollabSync - Local Buffer Overflow / Adobe Reader X Sandbox Bypass
(Metasploit) |
windows/local/[01;31m[K25[m[K7[01;31m[K25[m[K.rb

Adrenalin Player 2.2.5.3 - '.m3u' Local Buffer Overflow (SEH)
| windows/local/[01;31m[K25[m[K419.pl

Adrenalin Player 2.2.5.3 - '.wvx' Local Buffer Overflow (SEH)
| windows/local/265[01;31m[K25[m[K.py

Adult Tube Video Script - SQL Injection
| php/webapps/417[01;31m[K25[m[K.txt

Adult Video Site Script - Multiple Vulnerabilities
| php/webapps/118[01;31m[K25[m[K.html

Advanced Guestbook 2.3.1/2.4 - 'index.php?Entry' SQL Injection
| php/webapps/[01;31m[K25[m[K630.txt

Advanced Guestbook 2.4.0 - 'phpBB' Remote File Inclusion
| php/webapps/17[01;31m[K25[m[K.pl

Advanced Poll 2.0.2 - 'common.inc.php' Remote File Inclusion
| php/webapps/28[01;31m[K25[m[K3.txt

ae2 - 'standart.inc.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K13.txt

Affiliate Niche Script 3.4.0 - SQL Injection
| php/webapps/4[01;31m[K25[m[K27.txt

Affix Bluetooth Protocol Stack 3.1/3.2 - Signed Buffer Index (1)
| linux/dos/[01;31m[K25[m[K5[01;31m[K25[m[K.c

Affix Bluetooth Protocol Stack 3.1/3.2 - Signed Buffer Index (2)
| linux/remote/[01;31m[K25[m[K526.c

AFGB Guestbook 2.2 - 'Htmls' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K29.txt

Agent Tesla Botnet - Arbitrary Code Execution (Metasploit)
| php/remote/47[01;31m[K25[m[K6.rb

agorum core Pro 7.8.1.4-[01;31m[K25[m[K1 - Cross-Site Request Forgery
| multiple/webapps/41881.html

agorum core Pro 7.8.1.4-[01;31m[K25[m[K1 - Persistent Cross-Site
Scripting |
multiple/webapps/41882.html

AHG Search Engine 1.0 - 'search.cgi' Arbitrary Command Execution
| cgi/webapps/21[01;31m[K25[m[K7.txt

AIOCP 1.3.x - 'cp_forum_view.php' SQL Injection
| php/webapps/289[01;31m[K25[m[K.txt

Air Drive Plus 2.4 - Arbitrary File Upload
| ios/webapps/38[01;31m[K25[m[K8.txt

AirTies Air5341 Modem 1.0.0.12 - Cross-Site Request Forgery
| hardware/webapps/46[01;31m[K25[m[K3.html

Airties AIR5342 1.0.0.18 - Cross-Site Scripting
| hardware/webapps/455[01;31m[K25[m[K.txt

AIX 3.x/4.x / Windows 95/98/2000/NT 4.0 / SunOS 5 - 'gethostbyname()'
Remote Buffer Overflow |
multiple/remote/22[01;31m[K25[m[K1.sh

Ajax Availability Calendar 3.x - Multiple Vulnerabilities
| php/webapps/[01;31m[K25[m[K409.txt

akcms 4.2.4 - Information Disclosure
| php/webapps/21[01;31m[K25[m[K1.txt

Aladdin Knowledge System Ltd. PrivAgent ActiveX Control 2.0 - Multiple
Vulnerabilities |
windows/dos/22[01;31m[K25[m[K8.txt

Album Photo Sans Nom 1.6 - Remote Source Disclosure
| php/webapps/[01;31m[K25[m[K07.txt

Alcassoft's SOPHIA CMS - SQL Injection
| cfm/webapps/162[01;31m[K25[m[K.txt

Alfresco - '/cmisbrowser?url' Server-Side Request Forgery
| multiple/remote/39[01;31m[K25[m[K9.txt

Alfresco - '/proxy?endpoint' Server-Side Request Forgery
| multiple/remote/39[01;31m[K25[m[K8.txt

Alibaba Clone 3.0 (Special) - SQL Injection
| php/webapps/1[01;31m[K25[m[K43.rb

Alibaba Clone Diamond Version - SQL Injection
| php/webapps/1[01;31m[K25[m[K44.rb

ALiCE-CMS 0.1 - 'CONFIG[local_root]' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K82.txt

Alienvault Open Source SIEM (OSSIM) 4.1.2 - Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K447.txt

All Enthusiast PhotoPost PHP Pro 5.0 - 'adm-photo.php' Arbitrary Image
Manipulation |
php/webapps/[01;31m[K25[m[K208.txt

All In One 1.4 Control Panel - 'cp_polls_results.php' SQL Injection
| php/webapps/3[01;31m[K25[m[K37.txt

all-in-one-seo-pack 3.2.7 - Persistent Cross-Site Scripting
| php/webapps/474[01;31m[K25[m[K.txt

All4WWW-HomePageCreator 1.0 - 'index.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K422.txt

Allied Telesis AT-RG634A ADSL Broadband Router - Web Shell
| hardware/webapps/3[01;31m[K25[m[K45.txt

ALLMediaServer 0.8 - Remote Overflow (SEH)
| windows/remote/196[01;31m[K25[m[K.py

almond Classifieds ads - Blind SQL Injection / Cross-Site Scripting
| php/webapps/9[01;31m[K25[m[K9.txt

Aloaha Credential Provider Monitor 5.0.226 - Local Privilege Escalation
| windows/local/24[01;31m[K25[m[K8.txt

Alsbtain Bulletin 1.5/1.6 - Multiple Local File Inclusions
| php/webapps/36[01;31m[K25[m[K4.txt

ALSCO CMS - SQL Injection
| php/webapps/127[01;31m[K25[m[K.txt

Alstrasoft EPay Pro 2.0 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K328.txt

```
Alstrasoft EPay Pro 2.0 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K327.txt

Alstrasoft Template Seller Pro 3.[01;31m[K25[m[K - 'Fullview.php'
Cross-Site Scripting                                  |
php/webapps/27078.txt

Alstrasoft Template Seller Pro 3.[01;31m[K25[m[K - Admin Password
Change                                                |
php/webapps/3958.php

Alstrasoft Template Seller Pro 3.[01;31m[K25[m[K - Remote Code
Execution                                               |
php/webapps/3959.php

Alstrasoft Template Seller Pro 3.[01;31m[K25[m[K - Remote File
Inclusion                                               |
php/webapps/26515.txt

Alstrasoft Template Seller Pro 3.[01;31m[K25[m[Ke - 'tempid' SQL
Injection                                               |
php/webapps/41249.pl

Alt-N MDaemon 3.1.1 - Denial of Service
| windows/dos/202[01;31m[K25[m[K.pl

Alt-N MDaemon POP3 Server < 9.06 - 'USER' Remote Heap Overflow
| windows/remote/2[01;31m[K25[m[K8.py

Alt-N MDaemon WorldClient And WebAdmin - Cross-Site Request Forgery
| windows/remote/383[01;31m[K25[m[K.txt

Alt-N WebAdmin 2.0.x - Remote File Disclosure
| cgi/remote/2[01;31m[K25[m[K42.txt

Alt-N WebAdmin 2.0.x - Remote File Viewing
| cgi/remote/2[01;31m[K25[m[K41.txt

alt-n WebAdmin 3.0.2 - Multiple Vulnerabilities
| cgi/webapps/[01;31m[K25[m[K067.txt

Altenergy Power Control Software C1.2.5 - OS command injection
| hardware/webapps/513[01;31m[K25[m[K.py

Altiris Client 6.0.88 - Service Privilege Escalation
| windows/local/[01;31m[K25[m[K554.c

AmbiCom Blue Neighbors 2.50 build [01;31m[K25[m[K00 - BlueTooth Stack
Object Push Buffer Overflow                          |
multiple/dos/27094.txt

Amiti Antivirus [01;31m[K25[m[K.0.640 - Unquoted Service Path
| windows/local/47747.txt
```

```
AN HTTPD - 'CMDIS.dll' Remote Buffer Overflow (PoC)
| windows/dos/[01;31m[K25[m[K364.txt

AN HTTPD 1.42 - Arbitrary Log Content Injection
| windows/remote/[01;31m[K25[m[K365.txt

AN HTTPD 1.x - Count.pl Directory Traversal
| windows/remote/2[01;31m[K25[m[K15.txt

Angular-Base64-Upload Library 0.1.21 - Unauthenticated Remote Code
Execution (RCE)                          |
multiple/webapps/52[01;31m[K25[m[K3.py

AnnonceScriptHP 2.0 - '/admin/admin_config/Aide.php?email' Cross-Site
Scripting                                |
php/webapps/29[01;31m[K25[m[K1.txt

AnnonceScriptHP 2.0 - 'email.php?id' SQL Injection
| php/webapps/29[01;31m[K25[m[K2.txt

AnnonceScriptHP 2.0 - 'membre.dwt.php?email' Cross-Site Scripting
| php/webapps/29[01;31m[K25[m[K0.txt

AnnonceScriptHP 2.0 - 'voirannonce.php?no' SQL Injection
| php/webapps/29[01;31m[K25[m[K3.txt

Annuaire 1Two 1.0/1.1 - 'index.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K821.txt

AnotherPHPBook (APB) 1.3.0 - Authentication Bypass
| php/webapps/92[01;31m[K25[m[K.txt

Answerdev 1.0.3 - Account Takeover
| go/webapps/51[01;31m[K25[m[K7.py

Anti-Trojan Elite 4.2.1 - 'Atepmon.sys' IOCTL Request Local Overflow /
Local Privilege Escalation          |
windows/local/3[01;31m[K25[m[K72.txt

Anuko Time Tracker 1.19.23.53[01;31m[K25[m[K - CSV/Formula Injection
| php/webapps/49027.txt

AnyBurn 4.3 - Local Buffer Overflow (SEH)
| windows/local/460[01;31m[K25[m[K.py

AnyDesk 9.0.1 - Unquoted Service Path
| windows/local/52[01;31m[K25[m[K8.txt

AOL 9.5 - Phobos.Playlist 'Import()' Remote Buffer Overflow
(Metasploit)                                  |
windows/remote/11[01;31m[K25[m[K7.rb
```

```
AOL Instant Messenger 4.x/5.x - Smiley Icon Location Remote Denial of
Service                                  |
windows/dos/[01;31m[K25[m[K633.txt

AOL Instant Messenger AIM - goaway Overflow (Metasploit)
| windows/remote/165[01;31m[K25[m[K.rb

Apache 1.3.x - HTDigest Realm Command Line Argument Buffer Overflow (1)
| unix/remote/[01;31m[K25[m[K624.c

Apache 1.3.x - HTDigest Realm Command Line Argument Buffer Overflow (2)
| unix/remote/[01;31m[K25[m[K6[01;31m[K25[m[K.c

Apache CouchDB 1.5.0 - 'uuids' Denial of Service
| multiple/dos/3[01;31m[K25[m[K19.txt

Apache Mod_Access_Referer 1.0.2 - Null Pointer Dereference Denial of
Service                                   |
multiple/dos/2[01;31m[K25[m[K05.txt

Apache Spark - (Unauthenticated) Command Execution (Metasploit)
| java/remote/459[01;31m[K25[m[K.rb

Apache Struts - includeParams Remote Code Execution (Metasploit)
| multiple/remote/[01;31m[K25[m[K980.rb

Apache Tomcat 5 - Information Disclosure
| multiple/remote/28[01;31m[K25[m[K4.txt

Apache Tomcat 5.5.[01;31m[K25[m[K - Cross-Site Request Forgery
| multiple/webapps/29435.txt

Apache2Triad 1.5.4 - Multiple Vulnerabilities
| php/webapps/4[01;31m[K25[m[K20.txt

APC UPS 3.7.2 - 'apcupsd' Local Denial of Service
| linux/dos/[01;31m[K25[m[K1.c

APG Technology ClassMaster - Unauthorized Folder Access
| windows/remote/[01;31m[K25[m[K652.txt

Apple iOS < 10.3.1 - Kernel
| ios/local/4[01;31m[K25[m[K55.txt

Apple Mac OSX 10.10.5 - 'XNU' Local Privilege Escalation
| osx/local/378[01;31m[K25[m[K.txt

Apple Mac OSX 10.3.x - Multiple Vulnerabilities
| osx/local/[01;31m[K25[m[K[01;31m[K25[m[K6.c

Apple Mac OSX 10.x - BlueTooth Directory Traversal
| osx/remote/[01;31m[K25[m[K598.txt
```

Apple Mac OSX EvoCam Web Server (Snow Leopard) - ROP Remote Overflow
| osx/remote/14[01;31m[K25[m[K4.py

Apple Mac OSX Kernel - NULL Dereference in CoreCaptureResponder Due to
Unchecked Return Value | osx/dos/399[01;31m[K25[m[K.c

Apple Mac OSX Server - DirectoryService Buffer Overflow
| osx/dos/[01;31m[K25[m[K974.txt

Apple QuickTime 6.5.1 - PictureViewer Buffer Overflow
| windows/dos/[01;31m[K25[m[K281.py

Apple QuickTime RTSP 10.4.0 < 10.5.0 (OSX) - Content-Type Overflow
(Metasploit) |
osx/remote/99[01;31m[K25[m[K.rb

Apple Safari 10.1 - Spread Operator Integer Overflow Remote Code
Execution |
macos/remote/421[01;31m[K25[m[K.txt

Apple Safari 3.2.2/4b - nested elements XML Parsing Remote Crash
| windows/dos/83[01;31m[K25[m[K.py

Apple Safari 4.0.5 - 'parent.close()' Memory Corruption Code Execution
| windows/remote/1[01;31m[K25[m[K73.html

Apple watchOS 2 - Crash (PoC)
| hardware/dos/392[01;31m[K25[m[K.txt

Apple XNU Kernel - Memory Corruption due to Integer Overflow in
__offsetof Usage in posix_spawn on 32-bit |
multiple/dos/433[01;31m[K25[m[K.txt

Aqar Script 1.0 - Remote Bypass
| php/webapps/1[01;31m[K25[m[K67.html

Arcadem 2.01 - 'index.php' Remote File Inclusion
| php/webapps/305[01;31m[K25[m[K.txt

ardeaCore 2.[01;31m[K25[m[K - PHP Framework Remote File Inclusion
| php/webapps/15840.txt

Ariadne CMS 2.4 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K431.pl

Armida Databased Web Server 1.0 - GET Remote Denial of Service
| windows/dos/228[01;31m[K25[m[K.c

AROUNDMe 0.5.2 - 'templatePath' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K62.txt

Arq 5.10 - Local Privilege Escalation (1)
| macos/local/439[01;31m[K25[m[K.rb

```
Arris VAP[01;31m[K25[m[K00 - Authentication Bypass
| hardware/webapps/35372.rb

ArticleLive (Interspire Website Publisher) - SQL Injection
| asp/webapps/1[01;31m[K25[m[K26.txt

ASP Inline Corporate Calendar 3.6.3 - 'Defer.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K595.txt

ASP Inline Corporate Calendar 3.6.3 - 'Details.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K596.txt

ASP-DEV XM Forum RC3 - IMG Tag Script Injection
| asp/webapps/[01;31m[K25[m[K324.txt

ASP-Nuke 2.0.7 - 'gotourl.asp' Open Redirect
| asp/webapps/3[01;31m[K25[m[K80.txt

ASP2PHP 0.76.23 - Preparse Token Variable Buffer Overflow
| windows/remote/[01;31m[K25[m[K016.txt

ASPNuke 0.80 - 'Comments.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K498.txt

ASPNuke 0.80 - 'detail.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K500.txt

ASPNuke 0.80 - 'forgot_password.asp?email' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K905.txt

ASPNuke 0.80 - 'Language_Select.asp' HTTP Response Splitting
| asp/webapps/[01;31m[K25[m[K907.txt

ASPNuke 0.80 - 'profile.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K501.txt

ASPNuke 0.80 - 'register.asp' Multiple Cross-Site Scripting
Vulnerabilities                                 |
asp/webapps/[01;31m[K25[m[K906.txt

ASPNuke 0.80 - 'Select.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K502.txt

ASPPlayGround.NET 3.2 SR1 - Arbitrary File Upload
| asp/webapps/[01;31m[K25[m[K908.txt

Asterisk 1.0.12/1.2.12.1 - 'chan_skinny' Remote Heap Overflow (PoC)
| multiple/dos/[01;31m[K25[m[K97.pl

Astium VoIP PBX 2.1 build [01;31m[K25[m[K399 - Multiple
Vulnerabilities/Remote Command Execution                        |
php/webapps/23831.py
```

```
Astium VoIP PBX 2.1 build [01;31m[K25[m[K399 - Remote Crash (PoC)
| linux/dos/23830.py

AstroCMS - Multiple Vulnerabilities
| php/webapps/178[01;31m[K25[m[K.txt

Asus Dpcproxy - Remote Buffer Overflow (Metasploit)
| windows/remote/164[01;31m[K25[m[K.rb

Asus Precision TouchPad 11.0.0.[01;31m[K25[m[K - Denial of Service
| windows/dos/47322.py

Asus RT56U 3.0.0.4.360 - Remote Command Injection
| hardware/webapps/[01;31m[K25[m[K998.txt

Atheros Coex Service Application 8.0.0.[01;31m[K25[m[K5 - 'ZAtheros
Bt&Wlan Coex Agent' Unquoted Service Path           |
windows/local/49053.txt

Atom Photoblog 1.1.5b1 - 'photoId' SQL Injection
| php/webapps/61[01;31m[K25[m[K.txt

atrocore 1.5.[01;31m[K25[m[K User interaction - Unauthenticated File
upload - RCE                                        |
php/webapps/51271.txt

ATutor 1.4.3 - '/inbox/index.php?view' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K831.txt

ATutor 1.4.3 - 'browse.php?show_course' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K826.txt

ATutor 1.4.3 - 'contact.php?subject' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K827.txt

ATutor 1.4.3 - 'content.php?cid' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K828.txt

ATutor 1.4.3 - 'Directory.php' Multiple Cross-Site Scripting
Vulnerabilities                                     |
php/webapps/[01;31m[K25[m[K834.txt

ATutor 1.4.3 - 'search.php' Multiple Cross-Site Scripting
Vulnerabilities                                     |
php/webapps/[01;31m[K25[m[K830.txt

ATutor 1.4.3 - 'send_message.php?l' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K829.txt

ATutor 1.4.3 - 'subscribe_forum.php?us' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K833.txt
```

```
ATutor 1.4.3 - 'tile.php' Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K832.txt

ATutor 1.5.1 - 'password_reminder.php' SQL Injection
| php/webapps/26[01;31m[K25[m[K7.txt

ATutor 1.5.1 - Chat Logs Remote Information Disclosure
| php/webapps/26[01;31m[K25[m[K8.txt

AudioCoder - '.m3u' Local Buffer Overflow (Metasploit)
| windows/local/[01;31m[K25[m[K296.rb

AudioCoder 0.8.18 - Local Buffer Overflow (SEH)
| windows/local/[01;31m[K25[m[K141.rb

AudioCoder 0.8.29 - Memory Corruption (SEH)
| windows/local/3[01;31m[K25[m[K85.py

AuraCMS 2.2.1 - 'X-Forwarded-For' HTTP Header Blind SQL Injection
| php/webapps/5[01;31m[K25[m[K6.pl

AuraCMS Forum Module - SQL Injection
| php/webapps/4[01;31m[K25[m[K4.txt

AutoCar 1.1 - 'category' SQL Injection
| php/webapps/4[01;31m[K25[m[K62.txt

AutoIndex PHP Script 1.5.2 - 'index.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K940.txt

Automated Logic WebCTRL 6.1 - Path Traversal / Arbitrary File Write
| java/webapps/4[01;31m[K25[m[K43.txt

Automated Logic WebCTRL 6.5 - Local Privilege Escalation
| windows/local/4[01;31m[K25[m[K42.txt

Automated Logic WebCTRL 6.5 - Unrestricted File Upload / Remote Code
Execution                                |
java/webapps/4[01;31m[K25[m[K44.py

AV Arcade - 'Search' Cross-Site Scripting / HTML Injection
| php/webapps/1[01;31m[K25[m[K19.txt

Avast aswSnx.sys Kernel Driver 11.1.2[01;31m[K25[m[K3 - Memory
Corruption Privilege Escalation                          |
windows/dos/42182.cpp

AVCON H323Call - Local Buffer Overflow
| windows/local/1[01;31m[K25[m[K28.pl

AVE.CMS 2.09 - 'index.php?module' Blind SQL Injection
| php/webapps/[01;31m[K25[m[K716.py
```

```
AVerCaster Pro RS3400 Web Server - Directory Traversal
| hardware/webapps/2[01;31m[K25[m[K49.txt

Avira AntiVir Personal - Multiple Code Execution Vulnerabilities (1)
| windows/remote/352[01;31m[K25[m[K.c

Avira Internet Security - 'avipbb.sys' Filter Bypass / Privilege
Escalation                              |
windows/local/291[01;31m[K25[m[K.txt

AWCM - Database Disclosure
| php/webapps/110[01;31m[K25[m[K.txt

awiki 201001[01;31m[K25[m[K - Multiple Local File Inclusions
| php/webapps/36047.txt

AWStats 5.x/6.x - 'Logfile' Remote Command Execution
| cgi/webapps/[01;31m[K25[m[K108.txt

AWStats 5.x/6.x - Debug Remote Information Disclosure
| cgi/webapps/[01;31m[K25[m[K096.txt

AWStats 6.8 - 'AWStats.pl' Cross-Site Scripting
| cgi/webapps/32[01;31m[K25[m[K8.txt

AXIS Communications - Cross-Site Scripting / Content Injection
| hardware/webapps/416[01;31m[K25[m[K.txt

Axis Communications MPQT/PACS 5.20.x - Server-Side Include Daemon
Remote Format String                    |
multiple/remote/401[01;31m[K25[m[K.py

Ayukov NFTP FTP Client < 2.0 - Remote Buffer Overflow
| windows/remote/430[01;31m[K25[m[K.py

Azerbaijan Development Group AzDGDatingPlatinum 1.1.0 - 'view.php?id'
Cross-Site Scripting                |
php/webapps/[01;31m[K25[m[K373.txt

Azerbaijan Development Group AzDGDatingPlatinum 1.1.0 - 'view.php?id'
SQL Injection                       |
php/webapps/[01;31m[K25[m[K374.txt

Azure Apache Ambari 2302[01;31m[K25[m[K0400 - Spoofing
| multiple/remote/51546.py

B2B Classic Trading Script - 'offers.php' SQL Injection
| php/webapps/1[01;31m[K25[m[K32.txt

b2evolution 4.1.6 - Multiple Vulnerabilities
| php/webapps/[01;31m[K25[m[K298.txt
```

Back-End CMS 0.7.2.2 - 'BE_config.php' Remote File Inclusion
| php/webapps/18[01;31m[K25[m[K.txt

Backdrop Cms v1.[01;31m[K25[m[K.1 - Stored Cross-Site Scripting (XSS)
| php/webapps/51597.txt

Bahar Download Script 2.0 - 'aspkat.asp' SQL Injection
| asp/webapps/3[01;31m[K25[m[K00.txt

Bajie HTTP Server 0.95 - Example Scripts and Servlets Cross-Site
Scripting |
multiple/remote/23[01;31m[K25[m[K7.txt

BandSite CMS 1.1 - 'interview_content.php' Cross-Site Scripting
| php/webapps/286[01;31m[K25[m[K.txt

Banner Exchange Java - Authentication Bypass
| asp/webapps/74[01;31m[K25[m[K.txt

BaoFeng Storm - '.m3u' File Processing Buffer Overflow
| windows/local/1[01;31m[K25[m[K16.py

Base64 Decoder 1.1.2 - Local Buffer Overflow (SEH Egghunter)
| windows/local/466[01;31m[K25[m[K.py

Basic Analysis and Security Engine (BASE) 1.4.5 -
'base_qry_alert.php?base_path' Remote File Inclusion |
php/webapps/367[01;31m[K25[m[K.txt

BasiliX Webmail 1.1 - Email Header HTML Injection
| cgi/webapps/24[01;31m[K25[m[K4.txt

Battle Blog 1.[01;31m[K25[m[K - 'comment.asp' SQL Injection
| php/webapps/5731.txt

Battle Blog 1.[01;31m[K25[m[K - 'uploadform.asp' Arbitrary File Upload
| php/webapps/8647.txt

Battle Blog 1.[01;31m[K25[m[K - Authentication Bypass / SQL Injection /
HTML Injection | php/webapps/9183.txt

Battleaxe Software BTTLXE Forum - 'login.asp' SQL Injection
| asp/webapps/2[01;31m[K25[m[K29.txt

BBlog 0.7.4 - 'PostID' SQL Injection
| php/webapps/[01;31m[K25[m[K545.txt

bcoos 1.0.13 - 'click.php' SQL Injection
| php/webapps/3[01;31m[K25[m[K36.txt

bcoos 1.0.13 - 'common.php' Remote File Inclusion
| php/webapps/3[01;31m[K25[m[K32.txt

BEA WebLogic 7.0/8.1 - Administration Console Error Page Cross-Site Scripting |
jsp/webapps/[01;31m[K25[m[K739.txt

BEA WebLogic 7.0/8.1 - Administration Console LoginForm.jsp Cross-Site Scripting |
jsp/webapps/[01;31m[K25[m[K738.txt

BEA WebLogic Server 8.1 / WebLogic Express Administration Console - Cross-Site Scripting |
windows/remote/[01;31m[K25[m[K546.txt

BEdita 3.0.1.[01;31m[K25[m[K50 - Multiple Vulnerabilities
| php/webapps/15742.txt

Belkin F5D8233-4 Wireless N Router (Multiple Scripts) - Authentication Bypass |
hardware/remote/3[01;31m[K25[m[K82.txt

BetaParticle blog 2.0/3.0 - 'myFiles.asp' File Manipulation
| asp/webapps/[01;31m[K25[m[K[01;31m[K25[m[K4.txt

BetaParticle blog 2.0/3.0 - 'upload.asp' Arbitrary File Upload
| asp/webapps/[01;31m[K25[m[K[01;31m[K25[m[K3.txt

BetaParticle blog 2.0/3.0 - dbBlogMX.mdb Direct Request Database Disclosure |
asp/webapps/[01;31m[K25[m[K[01;31m[K25[m[K2.txt

Beyond Compare 3.0.13 b9599 - '.zip' Local Stack Buffer Overflow
| windows/local/1[01;31m[K25[m[K01.php

BFTPd 1.0.12 - Remote Overflow
| linux/remote/2[01;31m[K25[m[K.c

BibORB 1.3.2 - 'bibindex.php?search' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K118.txt

BibORB 1.3.2 - 'index.php' Traversal Arbitrary File Manipulation
| php/webapps/[01;31m[K25[m[K120.txt

BibORB 1.3.2 - Add Database 'Description' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K119.txt

BibORB 1.3.2 Login Module - Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K121.txt

big.asp - SQL Injection
| php/webapps/1[01;31m[K25[m[K33.txt

BigBlueButton 2.2.[01;31m[K25[m[K - Arbitrary File Disclosure and Server-Side Request Forgery |
multiple/webapps/49070.txt

```
BisonFTP 4R1 - Remote Denial of Service
| windows/dos/[01;31m[K25[m[K911.py

BitchX 1.0 - 'RPL_NAMREPLY' Denial of Service
| linux/dos/22[01;31m[K25[m[K9.c

Bitweaver 2.7 - 'fImg' Cross-Site Scripting
| php/webapps/34[01;31m[K25[m[K9.txt

Biz Mail Form 2.x - Unauthorized Mail Relay
| cgi/webapps/[01;31m[K25[m[K147.txt

BlaB! Lite 0.5 - Remote File Inclusion
| php/webapps/1[01;31m[K25[m[K91.txt

Black Knight Forum 4.0 - 'forum.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K505.txt

Black Knight Forum 4.0 - 'Member.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K504.txt

Bloggie Lite 0.0.2 Beta - Insecure Cookie Handling / SQL Injection
| php/webapps/69[01;31m[K25[m[K.txt

Blood Bank & Donor Management System 2.4 - CSRF Improper Input
Validation                                  |
multiple/webapps/52[01;31m[K25[m[K6.txt

Blue Coat Reporter 7.0/7.1 - License HTML Injection
| windows/remote/[01;31m[K25[m[K698.txt

Blue Coat Reporter 7.0/7.1 - Privilege Escalation
| windows/remote/[01;31m[K25[m[K697.txt

BlueSoleil 1.4 - Object Push Service BlueTooth Arbitrary File Upload /
Directory Traversal                 |
windows/remote/[01;31m[K25[m[K3[01;31m[K25[m[K.txt

BMForum 5.6 - 'index.php' Cross-Site Scripting
| php/webapps/318[01;31m[K25[m[K.txt

BOINC Manager (Seti@home) 7.0.64 - Field Buffer Overflow (SEH)
| windows/local/[01;31m[K25[m[K883.txt

BolinTech DreamFTP Server 1.02 - 'users.dat' Arbitrary File Disclosure
| windows/remote/85[01;31m[K25[m[K.pl

Bontago Game Server 1.1 - Remote Nickname Buffer Overrun
| multiple/remote/[01;31m[K25[m[K132.txt

Booking Centre 2.01 - 'HotelID' SQL Injection
| php/webapps/7[01;31m[K25[m[K3.txt
```

```
BookReview 1.0 - 'add_booklist.htm?node' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K731.txt

BookReview 1.0 - 'add_classification.htm?isbn' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K734.txt

BookReview 1.0 - 'add_contents.htm' Multiple Cross-Site Scripting
Vulnerabilities                          |
php/webapps/[01;31m[K25[m[K728.txt

BookReview 1.0 - 'add_review.htm' Multiple Cross-Site Scripting
Vulnerabilities                           |
php/webapps/[01;31m[K25[m[K727.txt

BookReview 1.0 - 'add_url.htm?node' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K732.txt

BookReview 1.0 - 'contact.htm?user' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K730.txt

BookReview 1.0 - 'search.htm?submit string' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K733.txt

BookReview 1.0 - 'suggest_category.htm?node' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K729.txt

BookReview 1.0 - 'suggest_review.htm?node' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K735.txt

Boonex Dolphin 5.2 - 'index.php' Remote Code Execution
| php/webapps/[01;31m[K25[m[K75.php

BOOTP Turbo 2.0.0.1[01;31m[K25[m[K3 - 'bootpt.exe' Unquoted Service
Path                                                |
windows/local/49851.txt

BoutikOne CMS - 'search_query' Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K88.txt

boxalino 09.05.[01;31m[K25[m[K-0421 - Directory Traversal
| multiple/webapps/9872.txt

Bravo Tejari Web Portal - Cross-Site Request Forgery
| multiple/webapps/44[01;31m[K25[m[K6.html

Brian Stanback bslist.cgi 1.0 - Remote Command Execution
| cgi/remote/205[01;31m[K25[m[K.txt

Brickcom IP Camera - Credentials Disclosure
| hardware/webapps/4[01;31m[K25[m[K88.txt

Brim 1.2.1 - 'renderer' Multiple Remote File Inclusions
| php/webapps/[01;31m[K25[m[K89.txt
```

```
Broadcom BCM43[01;31m[K25[m[K / BCM4329 Devices - Denial of Service
| hardware/dos/22739.py

Brooky CubeCart 2.0.1/2.0.4 - 'index.php?language' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K097.txt

Brooky CubeCart 2.0.1/2.0.4 - 'index.php?language' Traversal Arbitrary
File Access                          |
php/webapps/[01;31m[K25[m[K098.txt

BRS Webweaver 1.06 - HTTPd 'User-Agent' Remote Denial of Service
| multiple/dos/233[01;31m[K25[m[K.c

Bs Realtor_Web Script - SQL Injection
| php/webapps/142[01;31m[K25[m[K.txt

BS.Player 2.34 - '.bsl' Universal Overwrite (SEH)
| windows/local/8[01;31m[K25[m[K1.py

BSD / Linux - 'lpr' Local Privilege Escalation
| linux/local/3[01;31m[K25[m[K.c

BTCPay Server v1.7.4 - HTML Injection
| multiple/webapps/51[01;31m[K25[m[K4.txt

BuilderEngine 3.5.0 - Arbitrary File Upload and Execution (Metasploit)
| php/remote/420[01;31m[K25[m[K.rb

BulletProof FTP Client 2.45 - Remote Buffer Overflow
| windows/remote/[01;31m[K25[m[K30.py

Burning Board < 2.3.1 - SQL Injection
| php/webapps/438[01;31m[K25[m[K.txt

C'Nedra 0.4 Network Plugin - 'Read_TCP_String' Remote Buffer Overflow
| multiple/remote/[01;31m[K25[m[K710.txt

C.J. Steele Tattle - Remote Command Execution
| linux/remote/[01;31m[K25[m[K802.txt

C99Shell (Web Shell) - 'c99.php' Authentication Bypass
| php/webapps/340[01;31m[K25[m[K.txt

CA CAM (Windows x86) - 'log_security()' Remote Stack Buffer Overflow
(Metasploit)                         |
windows_x86/remote/168[01;31m[K25[m[K.rb

CA Release Automation NiMi 6.5 - Remote Command Execution
| java/remote/454[01;31m[K25[m[K.py

ca3de - Multiple Vulnerabilities
| multiple/remote/[01;31m[K25[m[K190.txt
```

Cacti 1.2.26 - Remote Code Execution (RCE) (Authenticated)
| php/webapps/522[01;31m[K25[m[K.txt

Cain & Abel 4.9.[01;31m[K25[m[K - 'Cisco IOS-MD5' Local Buffer Overflow
| windows/local/7688.pl

Calendarix 0.8.20071118 - Multiple SQL Injections / Cross-Site
Scripting Vulnerabilities |
php/webapps/[01;31m[K25[m[K778.txt

Camiro-CMS_beta-0.1 - 'FCKeditor' Arbitrary File Upload
| php/webapps/12[01;31m[K25[m[K1.php

CampSite 2.6.1 - 'g_documentRoot' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K60.txt

Captaris Infinite Mobile Delivery Webmail 2.6 - Full Path Disclosure
| php/webapps/[01;31m[K25[m[K071.txt

Car or Cab Booking Script - Authentication Bypass
| php/webapps/4[01;31m[K25[m[K82.txt

Car Portal 2.0 - 'car_make' Cross-Site Scripting
| php/webapps/350[01;31m[K25[m[K.html

Car Rental Management System 1.0 - SQL injection + Arbitrary File
Upload |
php/webapps/490[01;31m[K25[m[K.py

CarLine Forum Russian Board 4.2 - 'edit_msg.php' Multiple Cross-Site
Scripting Vulnerabilities |
php/webapps/[01;31m[K25[m[K885.txt

CarLine Forum Russian Board 4.2 - 'edit_msg.php?name_ig_array1[1]' SQL
Injection |
php/webapps/[01;31m[K25[m[K891.txt

CarLine Forum Russian Board 4.2 - 'enter.php' Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K895.txt

CarLine Forum Russian Board 4.2 - 'in.php' Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K894.txt

CarLine Forum Russian Board 4.2 - 'line.php' Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K893.txt

CarLine Forum Russian Board 4.2 - 'memory.php' Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K892.txt

CarLine Forum Russian Board 4.2 - 'menu_footer.php' Multiple Cross-Site
Scripting Vulnerabilities | php/webapps/[01;31m[K25[m[K876.txt

CarLine Forum Russian Board 4.2 - 'menu_header.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/[01;31m[K25[m[K878.txt

CarLine Forum Russian Board 4.2 - 'menu_header.php?table_sql' SQL Injection | php/webapps/[01;31m[K25[m[K886.txt

CarLine Forum Russian Board 4.2 - 'menu_tema.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/[01;31m[K25[m[K879.txt

CarLine Forum Russian Board 4.2 - 'new.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/[01;31m[K25[m[K884.txt

CarLine Forum Russian Board 4.2 - 'new.php?name_ig_array1[1]' SQL Injection | php/webapps/[01;31m[K25[m[K890.txt

CarLine Forum Russian Board 4.2 - 'reply.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/[01;31m[K25[m[K882.txt

CarLine Forum Russian Board 4.2 - 'reply.php?name_ig_array1[1]' SQL Injection | php/webapps/[01;31m[K25[m[K889.txt

CarLine Forum Russian Board 4.2 - 'reply_in.php' Multiple SQL Injections | php/webapps/[01;31m[K25[m[K888.txt

CarLine Forum Russian Board 4.2 - 'search.php?text_poisk' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K880.txt

CarLine Forum Russian Board 4.2 - 'set.php?name_ig_array[1]' SQL Injection | php/webapps/[01;31m[K25[m[K887.txt

CarLine Forum Russian Board 4.2 - 'set.php?name_ig_array[]' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K881.txt

CarLine Forum Russian Board 4.2 - IMG Tag Cross-Site Scripting | php/webapps/[01;31m[K25[m[K877.txt

Cart Engine 3.0.0 - 'task.php' Local File Inclusion | php/webapps/3[01;31m[K25[m[K04.txt

Cart Engine 3.0.0 - Database Backup Disclosure | php/webapps/3[01;31m[K25[m[K05.txt

Cart Engine 3.0.0 - Remote Code Execution
| php/webapps/3[01;31m[K25[m[K03.txt

CartWIZ 1.10 - 'Access.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K514.txt

CartWIZ 1.10 - 'AddToCart.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K506.txt

CartWIZ 1.10 - 'AddToWishlist.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K513.txt

CartWIZ 1.10 - 'error.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K515.txt

CartWIZ 1.10 - 'login.asp' Message Argument Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K520.txt

CartWIZ 1.10 - 'login.asp' Redirect Argument Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K516.txt

CartWIZ 1.10 - 'ProductCatalogSubCats.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K507.txt

CartWIZ 1.10 - 'ProductDetails.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K508.txt

CartWIZ 1.10 - 'searchresults.asp' idcategory Argument SQL Injection
| asp/webapps/[01;31m[K25[m[K511.txt

CartWIZ 1.10 - 'searchresults.asp' Name Argument Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K522.txt

CartWIZ 1.10 - 'searchresults.asp' PriceFrom Argument SQL Injection
| asp/webapps/[01;31m[K25[m[K510.txt

CartWIZ 1.10 - 'searchresults.asp' PriceTo Argument SQL Injection
| asp/webapps/[01;31m[K25[m[K509.txt

CartWIZ 1.10 - 'searchresults.asp' SKU Argument Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K521.txt

CartWIZ 1.10 - 'TellAFriend.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K512.txt

CDRTools CDRecord 1.11/2.0 - Devname Format String
| linux/local/2[01;31m[K25[m[K94.c

Cdsagenda 4.2.9 - 'SendAlertEmail.php' File Inclusion
| php/webapps/[01;31m[K25[m[K40.txt

CentiPaid 1.4.2 - 'centipaid_class.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K55.txt

```
CentOS Control Web Panel 0.9.8.838 - User Enumeration
| linux/webapps/471[01;31m[K25[m[K.txt

Centreo 19.10.8 - 'DisplayServiceStatus' Remote Code Execution
| php/webapps/48[01;31m[K25[m[K6.py

Centrify Deployment Manager 2.1.0.283 - Local Privilege Escalation
| linux/local/23[01;31m[K25[m[K1.txt

Cerberus FTP Server 2.1 - Information Disclosure
| windows/remote/2[01;31m[K25[m[K04.txt

Cerberus Helpdesk 0.97.3/2.6.1 - Multiple Cross-Site Scripting
Vulnerabilities                              |
php/webapps/[01;31m[K25[m[K803.txt

Cerulean Studios Trillian 3.0 - Remote '.png' Image File Parsing Buffer
Overflow                             |
windows/remote/[01;31m[K25[m[K181.py

CGI-Club imTRBBS 1.0 - Remote Command Execution
| cgi/webapps/[01;31m[K25[m[K918.txt

Chameleon LE 1.203 - 'index.php' Directory Traversal
| php/webapps/28[01;31m[K25[m[K5.txt

Chatness 2.5 - 'Message Form' HTML Injection
| php/webapps/[01;31m[K25[m[K315.html

Chatness 2.5.3 - '/options.php/save.php' Remote Code Execution
| php/webapps/37[01;31m[K25[m[K.php

Check Point VPN-1 SecureClient - IP Address Local Memory Access
| hardware/dos/[01;31m[K25[m[K107.txt

Check_MK 1.2.8p[01;31m[K25[m[K - Information Disclosure
| python/webapps/43021.py

Chicken of the VNC 2.0 - 'NULL-pointer' Remote Denial of Service
| osx/dos/3[01;31m[K25[m[K7.php

CHILKAT ASP String - 'CkString.dll 1.1 SaveToFile()' Insecure Method
| windows/remote/4[01;31m[K25[m[K5.html

Chrome V8 JIT - 'GetSpecializationContext' Type Confusion
| multiple/dos/44[01;31m[K25[m[K9.js

Chrome V8 JIT - JSBuiltinReducer::ReduceObjectCreate Fails to Ensure
that the Prototype is _null_          |
multiple/dos/44[01;31m[K25[m[K8.js
```

Chrome V8 JIT - Simplified-lowererer IrOpcode::kStoreField_
IrOpcode::kStoreElement Optimization Bug |
multiple/dos/44[01;31m[K25[m[K7.js

Ciamos 0.9.2 - 'Highlight.php' File Disclosure
| php/webapps/[01;31m[K25[m[K242.txt

Ciamos CMS 0.9.5 - 'module_path' Remote File Inclusion
| php/webapps/10[01;31m[K25[m[K9.txt

CIS WebServer 3.5.13 - Directory Traversal
| windows/remote/[01;31m[K25[m[K163.txt

Cisco - 'file' Directory Traversal
| hardware/remote/36[01;31m[K25[m[K6.txt

Cisco - Password Bruteforcer
| hardware/remote/[01;31m[K25[m[K4.c

Cisco ASA 8.x - 'EXTRABACON' Authentication Bypass
| hardware/remote/40[01;31m[K25[m[K8.txt

Cisco CallManager 1.0/2.0/3.x/4.0 - CTI Manager Remote Denial of
Service |
hardware/dos/[01;31m[K25[m[K967.txt

Cisco DPC2100 2.0.2 r1[01;31m[K25[m[K6-060303 - Multiple Security
Bypass / Cross-Site Request Forgery Vulnerabilities |
hardware/remote/34033.html

Cisco DPC2420 - Multiples Vulnerabilities
| hardware/webapps/23[01;31m[K25[m[K0.txt

Cisco EPC 39[01;31m[K25[m[K - Multiple Vulnerabilities
| asp/webapps/40383.txt

Cisco EPC39[01;31m[K25[m[K - Cross-Site Request Forgery
| hardware/webapps/30362.txt

Cisco EPC39[01;31m[K25[m[K - Persistent Cross-Site Scripting
| hardware/webapps/30415.txt

Cisco Linksys E4200 - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K25[m[K292.txt

Cisco Linksys WAG120N - Cross-Site Request Forgery
| hardware/webapps/16[01;31m[K25[m[K2.html

Cisco RV320 and RV3[01;31m[K25[m[K - Unauthenticated Remote Code
Execution (Metasploit) |
hardware/remote/46655.rb

Cisco VoIP Phone CP-7940 3.x - Spoofed SIP Status Message Handling
| hardware/remote/[01;31m[K25[m[K949.pl

Cisco WLC [01;31m[K25[m[K04 8.9 - Denial of Service (PoC)
| hardware/dos/47744.txt

CitrusDB 0.1/0.2/0.3 Credit Card Data - Remote Information Disclosure
| multiple/remote/[01;31m[K25[m[K072.txt

CitrusDB 0.3.6 - 'importcc.php' Arbitrary Database Injection
| php/webapps/[01;31m[K25[m[K099.txt

CitrusDB 0.3.6 - 'importcc.php' CSV File SQL Injection
| php/webapps/[01;31m[K25[m[K101.txt

CitrusDB 0.3.6 - 'uploadcc.php' Arbitrary Database Injection
| php/webapps/[01;31m[K25[m[K100.txt

CitrusDB 0.3.6 - Arbitrary Local PHP File Inclusion
| php/webapps/[01;31m[K25[m[K104.txt

CitrusDB 0.3.6 - Remote Authentication Bypass
| php/webapps/[01;31m[K25[m[K102.txt

CityPost PHP Image Editor M1/M2/M3/Imgsrc/M4 - 'URI' Cross-Site
Scripting |
php/webapps/[01;31m[K25[m[K459.txt

CityPost PHP LNKX 52.0 - 'message.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K458.txt

CityPost Simple PHP Upload - 'Simple-upload-53.php' Cross-Site
Scripting |
php/webapps/[01;31m[K25[m[K464.txt

CJ Ultra Plus 1.0.3/1.0.4 - 'OUT.php' SQL Injection
| php/webapps/[01;31m[K25[m[K623.txt

Clam AntiVirus 0.88.4 - 'rebuildpe' Remote Heap Overflow (PoC)
| multiple/dos/[01;31m[K25[m[K87.txt

Clam AntiVirus 0.88.4 - CHM Chunk Name Length Denial of Service (PoC)
| multiple/dos/[01;31m[K25[m[K86.pl

Claroline 1.5/1.6 - 'myagenda.php?coursePath' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K551.txt

Claroline 1.5/1.6 - 'toolaccess_details.php?tool' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K549.txt

Claroline 1.5/1.6 - 'user_access_details.php?data' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K550.txt

```
Claroline 1.8.0 rc1 - 'import.lib.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K10.txt

Claroline 1.8.3 - '$_SERVER['PHP_SELF']' Multiple Cross-Site Scripting
Vulnerabilities                      |
php/webapps/30[01;31m[K25[m[K9.txt

Claroline E-Learning 1.5/1.6 - 'exercises_details.php?exo_id' SQL
Injection                                |
php/webapps/[01;31m[K25[m[K553.txt

Claroline E-Learning 1.5/1.6 - 'userInfo.php' Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K552.txt

Clever Copy 2.0 - 'calendar.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K990.txt

Clever's Games Terminator 3: War of the Machines 1.16 Server - Remote
Buffer Overflow                       |
multiple/remote/[01;31m[K25[m[K708.txt

Clicksor - SQL Injection
| php/webapps/1[01;31m[K25[m[K00.txt

Clip Bucket 1.7.1 - Insecure Cookie Handling
| php/webapps/9[01;31m[K25[m[K5.txt

Clipbucket 2.4 RC2 645 - SQL Injection
| php/webapps/173[01;31m[K25[m[K.py

Clipbucket 2.6 - 'collections.php?cat' Cross-Site Scripting
| php/webapps/365[01;31m[K25[m[K.txt

Clipbucket 2.6 Revision 738 - Multiple SQL Injections
| php/webapps/23[01;31m[K25[m[K2.txt

ClipBucket < 4.0.0 - Release 4902 - Command Injection / File Upload /
SQL Injection                         |
php/webapps/44[01;31m[K25[m[K0.txt

ClipShare Pro 4.0 - 'fullscreen.php' Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K26.txt

CliServ Web Community 0.65 - 'cl_headers' Include
| php/webapps/2[01;31m[K25[m[K7.txt

Clone Script Directory Script 1.1.0 - 'cid' SQL Injection
| php/webapps/41[01;31m[K25[m[K9.txt

CloneCD/DVD 'ElbyCDIO.sys' < 6.0.3.2 - Local Privilege Escalation
| windows/local/8[01;31m[K25[m[K0.txt
```

```
CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)
| windows_x86-64/remote/46[01;31m[K25[m[K0.py

Cloudview NMS 2.00b - Writable Directory Traversal Execution
(Metasploit)                                    |
windows/remote/427[01;31m[K25[m[K.rb

CMS Web-Gooroo < 1.141 - Multiple Vulnerabilities
| php/webapps/4[01;31m[K25[m[K77.txt

CMScout 2.06 - SQL Injection / Local File Inclusion
| php/webapps/76[01;31m[K25[m[K.txt

CMSsite 1.0 - 'cat_id' SQL Injection
| php/webapps/46[01;31m[K25[m[K9.txt

Cobbler 2.4.x < 2.6.x - Local File Inclusion
| php/webapps/33[01;31m[K25[m[K2.txt

CoD2: DreamStats 4.2 - 'index.php' Remote File Inclusion
| php/webapps/3[01;31m[K25[m[K1.txt

CodeBlocks 12.11 (OSX) - Crash (PoC)
| osx/dos/[01;31m[K25[m[K809.py

Codefixer MailingListPro - Database Disclosure
| asp/webapps/73[01;31m[K25[m[K.txt

CodeThatShoppingCart 1.3.1 - 'catalog.php?id' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K637.txt

CodeThatShoppingCart 1.3.1 - 'catalog.php?id' SQL Injection
| php/webapps/[01;31m[K25[m[K638.txt

CodetoSell ViArt Shop Enterprise 2.1.6 - 'basket.php' Multiple Cross-
Site Scripting Vulnerabilities        |
php/webapps/[01;31m[K25[m[K575.txt

CodetoSell ViArt Shop Enterprise 2.1.6 - 'news_view.php' Multiple
Cross-Site Scripting Vulnerabilities     |
php/webapps/[01;31m[K25[m[K580.txt

CodetoSell ViArt Shop Enterprise 2.1.6 - 'page.php?page' Cross-Site
Scripting                                |
php/webapps/[01;31m[K25[m[K576.txt

CodetoSell ViArt Shop Enterprise 2.1.6 - 'products.php' Multiple Cross-
Site Scripting Vulnerabilities      |
php/webapps/[01;31m[K25[m[K579.txt

CodetoSell ViArt Shop Enterprise 2.1.6 -
'product_details.php?category_id' Cross-Site Scripting           |
php/webapps/[01;31m[K25[m[K578.txt
```

CodetoSell ViArt Shop Enterprise 2.1.6 - 'reviews.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/[01;31m[K25[m[K577.txt

ColdFusion 9-10 - Credential Disclosure | multiple/webapps/[01;31m[K25[m[K305.py

Collabtive 1.2 - Persistent Cross-Site Scripting | php/webapps/33[01;31m[K25[m[K0.txt

CombiWave Lite 4.0.1.4 - Denial of Service | windows/dos/146[01;31m[K25[m[K.py

Comdev eCommerce 3.0 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/[01;31m[K25[m[K062.txt

Comdev One Admin 4.1 - 'Adminfoot.php' Remote Code Execution | php/webapps/[01;31m[K25[m[K73.php

Comersus ASP Shopping Cart - File Disclosure / Cross-Site Scripting | asp/webapps/7[01;31m[K25[m[K9.txt

Comersus Cart 4.0/5.0 - 'Comersus_Search_Item.asp' Cross-Site Scripting | asp/webapps/[01;31m[K25[m[K390.txt

Comersus Cart 5.0/6.0 - Multiple Vulnerabilities | asp/webapps/[01;31m[K25[m[K060.txt

Comersus Open Technologies Comersus Cart 6.0.41 - Multiple Cross-Site Scripting Vulnerabilities | asp/webapps/[01;31m[K25[m[K956.txt

Comersus Open Technologies Comersus Cart 6.0.41 - Multiple SQL Injections | asp/webapps/[01;31m[K25[m[K953.txt

Commentics 2.0 - Multiple Vulnerabilities | php/webapps/193[01;31m[K25[m[K.txt

Community Link Pro - 'login.cgi?File' Remote Command Execution | cgi/webapps/[01;31m[K25[m[K920.pl

Community Server Forums - 'SearchResults.aspx' Cross-Site Scripting | asp/webapps/[01;31m[K25[m[K910.txt

CommunityPortals 1.0 - 'import-archive.php' File Inclusion | php/webapps/[01;31m[K25[m[K16.pl

Comodo Unified Threat Management Web Console 2.7.0 - Remote Code Execution | multiple/webapps/488[01;31m[K25[m[K.py

```
Company's Recruitment Management System 1.0 - 'Add New user' Cross-Site
Request Forgery (CSRF)             | php/webapps/504[01;31m[K25[m[K.txt

Compaq Client Management Agents 3.70/4.0 / Insight Management Agents
4.21 A/4.22 A/4.30 A / Intelligent Cl |
multiple/dos/192[01;31m[K25[m[K.txt

compop.ca 3.5.3 - Arbitrary code Execution
| multiple/webapps/52[01;31m[K25[m[K7.txt

Compro Technology IP Camera - ' index_MJpeg.cgi' Stream Disclosure
| hardware/webapps/50[01;31m[K25[m[K3.txt

Compro Technology IP Camera - ' mjpegStreamer.cgi' Screenshot
Disclosure                                  |
hardware/webapps/50[01;31m[K25[m[K4.txt

Compro Technology IP Camera - 'killps.cgi' Denial of Service (DoS)
| hardware/webapps/50[01;31m[K25[m[K0.txt

Compro Technology IP Camera - 'Multiple' Credential Disclosure
| hardware/webapps/50[01;31m[K25[m[K2.txt

Compro Technology IP Camera - RTSP stream disclosure (Unauthenticated)
| hardware/webapps/50[01;31m[K25[m[K1.txt

compteur 2.0 - 'param_editor.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K03.txt

Computalynx CProxy 3.3/3.4.x - Directory Traversal
| windows/remote/[01;31m[K25[m[K187.txt

COms - 'dynamic.php' Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K98.txt

Concrete CMS < 5.5.21 - Multiple Vulnerabilities
| php/webapps/372[01;31m[K25[m[K.pl

Concrete5 CMS < 5.4.2.1 - Multiple Vulnerabilities
| php/webapps/179[01;31m[K25[m[K.txt

ContaoCMS 2.10.1 - Cross-Site Scripting
| php/webapps/362[01;31m[K25[m[K.txt

ContentKeeper Web Appliance < 1[01;31m[K25[m[K.10 - Command Execution
(Metasploit)                                |
multiple/webapps/9916.rb

Conti FTP Server 1.0 - Large String Denial of Service
| windows/dos/30[01;31m[K25[m[K2.py

Control Web Panel 7 (CWP7) v0.9.8.1147 -  Remote Code Execution (RCE)
| php/webapps/51[01;31m[K25[m[K0.go
```

```
Convert-UUlib 1.04/1.05 Perl Module - Remote Buffer Overflow
| linux/remote/[01;31m[K25[m[K547.pl

Convex 3D 0.8 - Buffer Overflow
| windows/dos/[01;31m[K25[m[K007.txt

Cool Cafe Chat 1.2.1 - 'login.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K839.txt

Cool PDF Reader 3.0.2.[01;31m[K25[m[K6 - Buffer Overflow
| windows/dos/24463.txt

CoolForum 0.5/0.7/0.8 - 'avatar.php?img' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K239.txt

CoolForum 0.5/0.7/0.8 - 'register.php?login' SQL Injection
| php/webapps/[01;31m[K25[m[K240.txt

Coppermine Gallery 1.6.[01;31m[K25[m[K - RCE
| php/webapps/51738.txt

CoreFTP Server build 7[01;31m[K25[m[K - Directory Traversal
(Authenticated)                                                 |
windows/remote/50652.txt

Counter Strike: Condition Zero - '.BSP' Map File Code Execution
| windows/local/423[01;31m[K25[m[K.py

cPanel 10.8.x - 'cpwrap' via MySQLAdmin Privilege Escalation
| php/webapps/[01;31m[K25[m[K54.php

cPanel 11.[01;31m[K25[m[K - Cross-Site Request Forgery
| php/webapps/34[01;31m[K25[m[K5.html

cPanel 11.[01;31m[K25[m[K - Cross-Site Request Forgery (Add FTP
Account)                                                        |
php/webapps/14188.html

cPanel 11.[01;31m[K25[m[K Image Manager - 'target' Local File Inclusion
| php/webapps/34106.txt

cPanel 9.1 - 'User' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K846.txt

cPanel < 11.[01;31m[K25[m[K - Cross-Site Request Forgery (Add User PHP
Script)                                                         |
php/webapps/17330.html

cPanel and WHM 11.[01;31m[K25[m[K - 'failurl' HTTP Response Splitting
| php/webapps/33558.txt

CPG Dragonfly 9.0.2.0 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K316.txt
```

```
Craft CMS 3.0.[01;31m[K25[m[K - Cross-Site Scripting
| php/webapps/46054.txt

Craigslist Gold - SQL Injection
| php/webapps/[01;31m[K25[m[K247.txt

CSF Firewall - Buffer Overflow (PoC)
| linux/dos/182[01;31m[K25[m[K.c

CSV2XML 0.5.1 - Remote Buffer Overflow
| multiple/remote/[01;31m[K25[m[K028.txt

CubeCart 2.0.x - 'index.php' Multiple Full Path Disclosures
| php/webapps/[01;31m[K25[m[K355.txt

CubeCart 2.0.x - 'tellafriend.php?product' Full Path Disclosure
| php/webapps/[01;31m[K25[m[K356.txt

CubeCart 2.0.x - 'view_cart.php?add' Full Path Disclosure
| php/webapps/[01;31m[K25[m[K357.txt

CubeCart 2.0.x - 'view_product.php?product' Full Path Disclosure
| php/webapps/[01;31m[K25[m[K358.txt

CubeCart 2.0.x - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K162.txt

Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion
| php/webapps/[01;31m[K25[m[K971.txt

Curverider Elgg 1.0 - Templates HTML Injection
| php/webapps/348[01;31m[K25[m[K.html

CuteFTP 5.0 - Buffer Overflow
| windows_x86/local/45[01;31m[K25[m[K9.py

CuteNews 1.4.1 - 'show_news.php' Cross-Site Scripting
| php/webapps/27[01;31m[K25[m[K2.txt

CuteNews aj-fork - 'path' Remote File Inclusion
| php/webapps/3[01;31m[K25[m[K70.txt

CutePHP CuteNews 1.3.6 - 'x-forwarded-for' Script Injection
| php/webapps/[01;31m[K25[m[K177.txt

CyberBrau 0.9.4 - '/forum/track.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K59.txt

Cyberfolio 2.0 RC1 - 'av' Remote File Inclusion
| php/webapps/27[01;31m[K25[m[K.txt
```

Cyberoam Transparent Authentication Suite 2.1.2.5 - 'Fully Qualified Domain Name' Denial of Service (PoC) | windows/dos/469[01;31m[K25[m[K.py

CyberStrong EShop 4.2 - '10browse.asp' SQL Injection | asp/webapps/[01;31m[K25[m[K9[01;31m[K25[m[K.txt

CyberStrong eShop 4.2 - '10expand.asp' SQL Injection | asp/webapps/[01;31m[K25[m[K923.txt

CyberStrong EShop 4.2 - '20review.asp' SQL Injection | asp/webapps/[01;31m[K25[m[K922.txt

CyBoards PHP Lite 1.21/1.[01;31m[K25[m[K - 'Common.php' Remote File Inclusion | php/webapps/27970.txt

CyBoards PHP Lite 1.21/1.[01;31m[K25[m[K - 'post.php' SQL Injection | php/webapps/27422.txt

cyclades alterpath manager 1.1 - Multiple Vulnerabilities | jsp/webapps/[01;31m[K25[m[K159.txt

Cygnus Network Security 4.0/KerbNet 5.0 / MIT Kerberos 4/5 / RedHat 6.2 - Compatibility 'krb_rd_req()' Loc | linux/local/199[01;31m[K25[m[K.c

CzarNews 1.13/1.14 - 'headlines.php' Remote File Inclusion | php/webapps/[01;31m[K25[m[K244.txt

D-Forum 1 - 'footer' Remote File Inclusion | php/webapps/22[01;31m[K25[m[K7.txt

D-Forum 1 - 'header' Remote File Inclusion | php/webapps/22[01;31m[K25[m[K6.txt

D-Forum 1.11 - 'Nav.php3' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K185.txt

D-Link DAP-13[01;31m[K25[m[K - Broken Access Control | hardware/webapps/51556.txt

D-Link DCS-900 Camera - Remote IP Address Changer | hardware/remote/4[01;31m[K25[m[K.c

D-Link DIR-100 - Multiple Vulnerabilities | hardware/webapps/314[01;31m[K25[m[K.txt

D-Link DIR-600 - Authentication Bypass | hardware/webapps/4[01;31m[K25[m[K81.txt

D-Link DIR-600M - Authentication Bypass (Metasploit) | hardware/webapps/47[01;31m[K25[m[K0.rb

D-Link DIR-615H - OS Command Injection (Metasploit)
| hardware/remote/[01;31m[K25[m[K609.rb

D-Link DIR-635 - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K25[m[K024.txt

D-Link DIR-8[01;31m[K25[m[K (vC) - Multiple Vulnerabilities
| hardware/remote/38718.txt

D-Link DIR-880L - Multiple Buffer Overflow Vulnerabilities
| hardware/remote/387[01;31m[K25[m[K.txt

D-Link DNS-323 - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K25[m[K142.txt

D-Link DNS-3[01;31m[K25[m[K ShareCenter < 1.05B03 - Multiple
Vulnerabilities |
php/webapps/43846.txt

D-Link DSL Router - Remote Authentication Bypass
| hardware/remote/[01;31m[K25[m[K684.html

D-Link DSL-320B - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K25[m[K[01;31m[K25[m[K1.txt

D-Link DSR-[01;31m[K25[m[K0N 3.12 - Denial of Service (PoC)
| hardware/webapps/48863.txt

D-Link IP Cameras - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K25[m[K138.txt

daChooch - SQL Injection
| php/webapps/114[01;31m[K25[m[K.txt

damianov.net Shoutbox - Cross-Site Scripting
| php/webapps/1[01;31m[K25[m[K93.txt

Dark Hart Portal - 'login.php' Remote File Inclusion
| php/webapps/1[01;31m[K25[m[K53.txt

Darwin Kernel 7.1 - Mach File Parsing Local Integer Overflow
| osx/local/[01;31m[K25[m[K055.c

DATAC RealWin - Multiple Vulnerabilities
| windows/dos/170[01;31m[K25[m[K.txt

DATAC RealWin SCADA Server 2.0 (Build 6.1.8.10) - Buffer Overflow
| windows/dos/15[01;31m[K25[m[K9.txt

Datenbank Module For phpBB - 'Remote mod.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K433.txt

```
Dating Script 3.[01;31m[K25[m[K - SQL Injection
| php/webapps/41027.txt

dB Masters Curium CMS 1.03 - 'c_id' SQL Injection
| php/webapps/3[01;31m[K25[m[K6.txt

DCP-Portal 6.1.1 - Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K109.txt

Debian 2.1 - HTTPd
| linux/remote/19[01;31m[K25[m[K3.txt

Debian 2.1/2.2 / Mandrake 6.0/6.1/7.0 / RedHat 6.x - 'rpc.lockd' Remote
Denial of Service                  | linux/dos/200[01;31m[K25[m[K.txt

deeemm CMS (dmcms) 0.7.4 - Multiple Vulnerabilities
| php/webapps/6[01;31m[K25[m[K0.txt

Deepin TFTP Server 1.[01;31m[K25[m[K - Directory Traversal
| windows/remote/14779.pl

Def-Blog 1.0.3 - 'comadd.php' SQL Injection
| php/webapps/[01;31m[K25[m[K67.txt

Dell SonicWALL EMail Security Appliance Application 7.4.5 - Multiple
Vulnerabilities                        |
multiple/webapps/3[01;31m[K25[m[K56.txt

DELTAScripts PHP Shop 1.0 - Authentication Bypass
| php/webapps/70[01;31m[K25[m[K.txt

Deonixscripts Templates Management 1.3 - SQL Injection
| php/webapps/9[01;31m[K25[m[K1.txt

Desi Short URL Script - (Authentication Bypass) Insecure Cookie
Handling                                  |
php/webapps/89[01;31m[K25[m[K.txt

Dev Web Manager System 1.5 - 'index.php' Cross-Site Scripting
| php/webapps/288[01;31m[K25[m[K.txt

Device Monitoring Studio 8.10.00.89[01;31m[K25[m[K - Denial of Service
(PoC)                                              | windows/dos/46321.py

devolo dLAN 550 duo+ Starter Kit - Remote Code Execution
| hardware/webapps/463[01;31m[K25[m[K.txt

DeWorkshop 1.0 - Arbitrary File Upload
| php/webapps/4[01;31m[K25[m[K04.txt

DHCart 3.84 - Multiple Cross-Site Scripting / HTML Injection
Vulnerabilities                                |
php/webapps/3[01;31m[K25[m[K67.txt
```

Digital College 1.0 - Arbitrary File Upload
| php/webapps/1[01;31m[K25[m[K68.txt

DigitalHive 2.0 - 'membres.php?mt' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K264.txt

DigitalHive 2.0 - 'msg.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K263.txt

DigitalHive 2.0 RC2 - 'base_include.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K66.txt

DirectContact 0.3.b - Directory Traversal
| windows/remote/273[01;31m[K25[m[K.txt

DirectTopics 2 - 'topic.php' SQL Injection
| php/webapps/[01;31m[K25[m[K653.txt

Disk Pulse Enterprise 9.9.16 - 'Import Command' Local Buffer Overflow
| windows/local/4[01;31m[K25[m[K36.py

Disk Pulse Enterprise 9.9.16 - Remote Buffer Overflow (SEH)
| windows/remote/4[01;31m[K25[m[K60.py

Disk Savvy Enterprise 9.9.14 - 'Import Command' Local Buffer Overflow
| windows/local/4[01;31m[K25[m[K38.py

Disk Savvy Enterprise 9.9.14 - Remote Buffer Overflow (SEH)
| windows/remote/4[01;31m[K25[m[K58.py

DivX Player 2.6 - '.Skin' File Directory Traversal
| windows/remote/[01;31m[K25[m[K057.txt

Dizi Portali - 'film.asp' SQL Injection
| asp/webapps/3[01;31m[K25[m[K77.txt

DJ Legend 6.01 - Denial of Service
| windows/dos/15[01;31m[K25[m[K8.py

djbdns 1.05 - Long Response Packet Remote Cache Poisoning
| linux/remote/328[01;31m[K25[m[K.txt

DjVuLibre 3.5.[01;31m[K25[m[K.3 - Out of Bounds Access Violation
| windows/dos/34135.py

DNSTools 2.0 - Authentication Bypass
| php/webapps/214[01;31m[K25[m[K.txt

DO-CMS - Multiple SQL Injections
| php/webapps/16[01;31m[K25[m[K6.txt

Dokeos 1.x - '/forum/viewforum.php?forum' Cross-Site Scripting
| php/webapps/309[01;31m[K25[m[K.txt

```
dokuwiki 2009-12-[01;31m[K25[m[K - Multiple Vulnerabilities
| php/webapps/11141.txt

Dolibarr ERP/CRM < 3.2.0 / < 3.1.1 - OS Command Injection
| php/webapps/187[01;31m[K25[m[K.txt

Dolphin 2.0 - '.elf' Local Denial of Service
| windows/dos/1[01;31m[K25[m[K41.php

Domain Quester Pro 6.02 - Stack Overflow (SEH)
| windows/local/478[01;31m[K25[m[K.py

DomainMod 4.13 - Cross-Site Scripting
| php/webapps/473[01;31m[K25[m[K.txt

Dorsa CMS - 'Default_.aspx' Cross-Site Scripting
| asp/webapps/3[01;31m[K25[m[K49.txt

DotA OpenStats 1.3.9 - SQL Injection
| php/webapps/18[01;31m[K25[m[K0.txt

DotBr 0.1 - 'Exec.php3' Remote Command Execution
| php/webapps/22[01;31m[K25[m[K4.txt

DotBr 0.1 - 'System.php3' Remote Command Execution
| php/webapps/22[01;31m[K25[m[K3.txt

dotclear 2.[01;31m[K25[m[K.3 - Remote Code Execution (RCE)
(Authenticated)                                                 |
php/webapps/51353.txt

dotCMS 5.1.1 - HTML Injection
| jsp/webapps/468[01;31m[K25[m[K.txt

DotNetNuke 9.5 - File Upload Restrictions Bypass
| aspx/webapps/481[01;31m[K25[m[K.txt

dotProject 2.0 - '/modules/tasks/gantt.php?baseDir' Remote File
Inclusion                                       |
php/webapps/272[01;31m[K25[m[K.txt

Double Choco Latte 0.9.3/0.9.4 - 'main.php' Arbitrary PHP Code
Execution                                        |
php/webapps/[01;31m[K25[m[K271.txt

Dovecot 1.1.x - Invalid Message Address Parsing Denial of Service
| linux/dos/3[01;31m[K25[m[K51.txt

Dovecot IMAP 1.0.10 < 1.1rc2 - Remote Email Disclosure
| multiple/remote/5[01;31m[K25[m[K7.py

Dovecot with Exim - 'sender_address' Remote Command Execution
| linux/remote/[01;31m[K25[m[K297.txt
```

```
Download-Engine 1.4.2 - 'spaw' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K21.txt

Dragonfly Commerce 1.0 - Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K963.txt

Dream Vision Technologies Web Portal - SQL Injection
| php/webapps/171[01;31m[K25[m[K.txt

Dream4 Koobi CMS 4.2.3 - 'index.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K272.txt

Dream4 Koobi CMS 4.2.3 - 'index.php' SQL Injection
| php/webapps/[01;31m[K25[m[K273.txt

Dream4 Koobi CMS 4.2.3 - 'index.php?P' SQL Injection
| php/webapps/[01;31m[K25[m[K555.txt

Dream4 Koobi CMS 4.2.3 - 'index.php?Q' SQL Injection
| php/webapps/[01;31m[K25[m[K556.txt

Dream4 Koobi Pro 6.[01;31m[K25[m[K Gallery - 'galid' SQL Injection
| php/webapps/5413.txt

Dream4 Koobi Pro 6.[01;31m[K25[m[K Links - 'categ' SQL Injection
| php/webapps/5411.txt

Dream4 Koobi Pro 6.[01;31m[K25[m[K Poll - 'poll_id' SQL Injection
| php/webapps/5448.txt

Dream4 Koobi Pro 6.[01;31m[K25[m[K Shop - 'categ' SQL Injection
| php/webapps/5412.txt

Dream4 Koobi Pro 6.[01;31m[K25[m[K Showimages - 'galid' SQL Injection
| php/webapps/5414.txt

Drupal Module CKEditor < 4.1WYSIWYG (Drupal 6.x/7.x) - Persistent
Cross-Site Scripting                    |
php/webapps/[01;31m[K25[m[K493.txt

DS3 Authentication Server - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K25[m[K976.txt

Dualis 20.4 - '.bin' Local Denial of Service
| windows/dos/120[01;31m[K25[m[K.php

DUClassmate 1.x - 'ICity' SQL Injection
| asp/webapps/30[01;31m[K25[m[K0.txt

Dup Scout 13.5.28 - 'Multiple' Unquoted Service Path
| windows/local/500[01;31m[K25[m[K.txt
```

Dup Scout Enterprise 9.9.14 - Remote Buffer Overflow (SEH)
| windows/remote/4[01;31m[K25[m[K57.py

DUportal 3.1.2 - 'channel.asp?iChannel' SQL Injection
| asp/webapps/[01;31m[K25[m[K482.txt

DUportal 3.1.2 - 'inc_poll_voting.asp?DAT_PARENT' SQL Injection
| asp/webapps/[01;31m[K25[m[K483.txt

DUportal 3.1.2 - 'inc_rating.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K484.txt

DUportal 3.1.2 - 'type.asp?iCat' SQL Injection
| asp/webapps/[01;31m[K25[m[K485.txt

DUportal Pro 3.4 - 'cat.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K480.txt

DUportal Pro 3.4 - 'default.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K476.txt

DUportal Pro 3.4 - 'detail.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K481.txt

DUportal Pro 3.4 - 'inc_vote.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K478.txt

DUportal Pro 3.4 - 'result.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K479.txt

DUportal Pro 3.4 - 'search.asp?iChannel' SQL Injection
| asp/webapps/[01;31m[K25[m[K477.txt

DUware DUamazon Pro 3.0/3.1 - 'catDelete.asp?iCat' SQL Injection
| asp/webapps/[01;31m[K25[m[K863.txt

DUware DUamazon Pro 3.0/3.1 - 'detail.asp?iSub' SQL Injection
| asp/webapps/[01;31m[K25[m[K865.txt

DUware DUamazon Pro 3.0/3.1 - 'productDelete.asp?iCat' SQL Injection
| php/webapps/[01;31m[K25[m[K861.txt

DUware DUamazon Pro 3.0/3.1 - 'productEdit.asp?iCat' SQL Injection
| php/webapps/[01;31m[K25[m[K862.txt

DUware DUamazon Pro 3.0/3.1 - 'review.asp?iPro' SQL Injection
| asp/webapps/[01;31m[K25[m[K864.txt

DUware DUamazon Pro 3.0/3.1 - 'type.asp?iType' SQL Injection
| php/webapps/[01;31m[K25[m[K860.txt

DUware DUclassmate 1.x - 'default.asp?iState' SQL Injection
| asp/webapps/[01;31m[K25[m[K872.txt

DUware DUclassmate 1.x - 'edit.asp?iPro' SQL Injection
| asp/webapps/[01;31m[K25[m[K873.txt

DUware DUforum 3.0/3.1 - 'forums.asp?iFor' SQL Injection
| asp/webapps/[01;31m[K25[m[K870.txt

DUware DUforum 3.0/3.1 - 'messages.asp?iMsg' SQL Injection
| asp/webapps/[01;31m[K25[m[K868.txt

DUware DUforum 3.0/3.1 - 'post.asp?iFor' SQL Injection
| asp/webapps/[01;31m[K25[m[K869.txt

DUware DUforum 3.0/3.1 - 'userEdit.asp?id' SQL Injection
| asp/webapps/[01;31m[K25[m[K871.txt

DUware DUpaypal 3.0/3.1 - 'detail.asp?iPro' SQL Injection
| asp/webapps/[01;31m[K25[m[K866.txt

DUware DUpaypal 3.0/3.1 - 'sub.asp?iSub' SQL Injection
| asp/webapps/[01;31m[K25[m[K867.txt

DUware DUportal 3.4.3 Pro - Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K858.txt

DVBBS 7.1 - 'ShowErr.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K965.txt

DVD-Lab Studio 1.[01;31m[K25[m[K - '.DAL' File Open Crash
| windows/dos/18903.rb

Dynamic Biz Website Builder (QuickWeb) 1.0 - 'login.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K914.txt

E-Uploader Pro 1.0 - Image Upload / Code Execution
| php/webapps/[01;31m[K25[m[K56.txt

e-webtech - 'fixed_page.asp' SQL Injection
| php/webapps/1[01;31m[K25[m[K83.txt

e-webtech - 'new.asp?id=' SQL Injection
| php/webapps/1[01;31m[K25[m[K47.txt

e-webtech - 'page.asp' SQL Injection
| asp/webapps/1[01;31m[K25[m[K71.txt

e107 0.7.16 - Referer header Cross-Site Scripting
| php/webapps/98[01;31m[K25[m[K.txt

e107 0.7.24 - 'cmd' Remote Command Execution
| php/webapps/36[01;31m[K25[m[K2.txt

e107 0.7.[01;31m[K25[m[K - 'news.php' SQL Injection
| php/webapps/35709.txt

```
e107 0.7.x - CAPTCHA Security Bypass / Cross-Site Scripting
| php/webapps/33[01;31m[K25[m[K6.txt

e107 < 0.6172 - 'resetcore.php' SQL Injection
| linux/remote/1[01;31m[K25[m[K8.php

e107 Website System 0.6 - Nested BBCode URL Tag Script Injection
| php/webapps/[01;31m[K25[m[K995.txt

e107 Website System 0.617 - 'Forum_viewforum.php' SQL Injection
| php/webapps/[01;31m[K25[m[K645.txt

e107 Website System 0.617 - 'Request.php' Directory Traversal
| php/webapps/[01;31m[K25[m[K644.txt

Early Impact ProductCart 2.6/2.7 - 'editCategories.asp?lid' SQL
Injection                                  |
asp/webapps/[01;31m[K25[m[K796.txt

Early Impact ProductCart 2.6/2.7 - 'modCustomCardPaymentOpt.asp?idc'
SQL Injection                           |
asp/webapps/[01;31m[K25[m[K797.txt

Early Impact ProductCart 2.6/2.7 - 'OptionFieldsEdit.asp?idccr' SQL
Injection                                  |
asp/webapps/[01;31m[K25[m[K798.txt

Early Impact ProductCart 2.6/2.7 - 'viewPrd.asp?idcategory' SQL
Injection                                  |
asp/webapps/[01;31m[K25[m[K795.txt

Ease Jukebox 1.30 - Denial of Service
| windows/dos/15[01;31m[K25[m[K0.py

Easy AVI DivX Converter 1.2.24 - Local Buffer Overflow (SEH)
| windows/local/4[01;31m[K25[m[K49.py

Easy DVD Creater 2.5.11 - Local Buffer Overflow (SEH)
| windows/local/4[01;31m[K25[m[K21.py

Easy DVD Creator 2.5.11 - Local Buffer Overflow (SEH)
| windows/local/4[01;31m[K25[m[K65.py

Easy File Sharing HTTP Server 7.2 - POST Buffer Overflow (Metasploit)
| windows/remote/42[01;31m[K25[m[K6.rb

Easy File Sharing Web Server 1.[01;31m[K25[m[K - Denial of Service
| windows/dos/423.pl

Easy FileManager 1.1 iOS - Multiple Vulnerabilities
| ios/webapps/3[01;31m[K25[m[K59.txt
```

Easy Icon Maker 5.01 - Crash (PoC)
| windows/dos/[01;31m[K25[m[K128.txt

Easy Message Board - Directory Traversal
| cgi/webapps/[01;31m[K25[m[K632.txt

Easy Message Board - Remote Command Execution
| cgi/webapps/[01;31m[K25[m[K634.txt

Easy RM RMVB to DVD Burner 1.8.11 - Local Buffer Overflow (SEH)
| windows/local/4[01;31m[K25[m[K68.py

Easy RM to MP3 Converter 2.7.3.700 - 'Input' Local Buffer Overflow
(SEH) |
windows/local/48[01;31m[K25[m[K7.py

Easy Software Products LPPassWd 1.1.22 - Resource Limit Denial of
Service |
windows/dos/[01;31m[K25[m[K012.c

Easy Vedio to PSP Converter 1.6.20 - Local Buffer Overflow (SEH)
| windows/local/4[01;31m[K25[m[K86.py

Easy Video to iPod Converter 1.6.20 - Buffer Overflow (SEH)
| windows/local/46[01;31m[K25[m[K5.py

Easy Video to iPod/MP4/PSP/3GP Converter 1.5.20 - Local Buffer Overflow
(SEH) |
windows/local/4[01;31m[K25[m[K48.py

Easy Web Search 4.0 - SQL Injection
| php/webapps/4[01;31m[K25[m[K72.txt

Easy WMV/ASF/ASX to DVD Burner 2.3.11 - Local Buffer Overflow (SEH)
| windows/local/4[01;31m[K25[m[K67.py

EasyCom For PHP 4.0.0 - Buffer Overflow (PoC)
| windows/dos/414[01;31m[K25[m[K.txt

Easyedit CMS - 'news.php?intPageID' SQL Injection
| php/webapps/3[01;31m[K25[m[K94.txt

Easyedit CMS - 'page.php?intPageID' SQL Injection
| php/webapps/3[01;31m[K25[m[K93.txt

Easyedit CMS - 'subcategory.php?intSubCategoryID' SQL Injection
| php/webapps/3[01;31m[K25[m[K92.txt

EasyMail Objects 6.0.2.0 - 'emimap4.dll' ActiveX Control Remote Code
Execution |
windows/dos/332[01;31m[K25[m[K.html

Easynews 4.4.1 - 'admin.php' Authentication Bypass
| php/webapps/[01;31m[K25[m[K88.txt

EasyPHPCalendar 6.1.5/6.2.x - 'calendar.php?serverPath' Remote File Inclusion |
php/webapps/[01;31m[K25[m[K928.txt

EasyPHPCalendar 6.1.5/6.2.x - 'datePicker.php?serverPath' Remote File Inclusion |
php/webapps/[01;31m[K25[m[K931.txt

EasyPHPCalendar 6.1.5/6.2.x - 'header.inc.php?serverPath' Remote File Inclusion |
php/webapps/[01;31m[K25[m[K930.txt

EasyPHPCalendar 6.1.5/6.2.x - 'popup.php?serverPath' Remote File Inclusion |
php/webapps/[01;31m[K25[m[K929.txt

EasyPHPCalendar 6.1.5/6.2.x - 'setupSQL.php?serverPath' Remote File Inclusion |
php/webapps/[01;31m[K25[m[K932.txt

Ebay Clone 2009 - Multiple SQL Injections
| php/webapps/91[01;31m[K25[m[K.txt

eboli - 'index.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K04.txt

ECK Hotel 1.0 - Cross-Site Request Forgery (Add Admin)
| php/webapps/48[01;31m[K25[m[K8.txt

ecoCMS 18.4.2010 - 'admin.php' Cross-Site Scripting
| php/webapps/339[01;31m[K25[m[K.txt

ECommPro 3.0 - 'Admin/login.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K466.txt

EdmoBBS 0.9 - SQL Injection
| php/webapps/266[01;31m[K25[m[K.txt

eFiction < 2.0.7 - Remote Admin Authentication Bypass
| php/webapps/2[01;31m[K25[m[K5.txt

eFront 3.6.10 - 'professor.php' Script Multiple SQL Injections
| php/webapps/36[01;31m[K25[m[K9.txt

EggBlog 4.1.2 - Arbitrary File Upload
| php/webapps/[01;31m[K25[m[K126.txt

eGroupWare 1.0 - '/sitemgr-site/index.php?category_id' Cross-Site Scripting |
php/webapps/[01;31m[K25[m[K435.txt

```
eGroupWare 1.0 - '/tts/index.php?filter' SQL Injection
| php/webapps/[01;31m[K25[m[K436.txt

eGroupWare 1.0 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                                    |
php/webapps/[01;31m[K25[m[K434.txt

eGroupWare 1.0 - 'index.php?cats_app' SQL Injection
| php/webapps/[01;31m[K25[m[K437.txt

EJ3 TOPo 2.2 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                                     |
php/webapps/[01;31m[K25[m[K689.txt

Elantech-Smart Pad 11.9.0.0 - Unquoted Service Path Privilege
Escalation                                         |
windows/local/404[01;31m[K25[m[K.txt

Elecard AVC_HD/MPEG Player 5.7 - Local Buffer Overflow
| windows/local/16[01;31m[K25[m[K3.py

Elemental Software CartWIZ 1.20 - Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K951.txt

elFinder 2 - Remote Command Execution (via File Creation)
| php/webapps/369[01;31m[K25[m[K.py

Elkagroup Image Gallery 1.0 - 'view.php' SQL Injection
| php/webapps/3[01;31m[K25[m[K42.txt

Eltek SmartPack - Backdoor Account
| hardware/webapps/42[01;31m[K25[m[K2.txt

eM Client e-mail client 5.0.180[01;31m[K25[m[K.0 - Persistent Cross-
Site Scripting                                      |
windows/remote/28183.py

EMC NetWorker - Format String (Metasploit)
| windows/remote/2[01;31m[K25[m[K[01;31m[K25[m[K.rb

eMerge E3 Access Controller 4.6.07 - Remote Code Execution
| hardware/remote/476[01;31m[K25[m[K.py

eNdonesia 8.4 - 'mod.php?viewarticle Action artid' SQL Injection
| php/webapps/302[01;31m[K25[m[K.txt

Enlightenment v0.[01;31m[K25[m[K.3 - Privilege escalation
| linux/local/51180.txt

Envolution 1.1.0 - 'topic' SQL Injection
| php/webapps/4[01;31m[K25[m[K6.pl
```

EO Video 1.36 - Local Heap Overflow Denial of Service / (PoC)
| windows/dos/6[01;31m[K25[m[K3.py

ePhone Disk 1.0.2 iOS - Multiple Vulnerabilities
| ios/webapps/3[01;31m[K25[m[K60.txt

EPNadmin 0.7 - 'constantes.inc.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K96.pl

EQdkp 1.3.1 - 'Referer Spoof' Remote Database Backup
| php/webapps/3[01;31m[K25[m[K2.txt

eRoom 6.0 PlugIn - Insecure File Download Handling
| cgi/webapps/[01;31m[K25[m[K950.pl

ERPNext 12.29 - Cross-Site Scripting (XSS)
| java/webapps/51[01;31m[K25[m[K5.txt

ERS Viewer 2011 - '.ERS' File Handling Buffer Overflow (Metasploit)
| windows/local/[01;31m[K25[m[K448.rb

escripts software e_board 4.0 - Directory Traversal
| cgi/webapps/[01;31m[K25[m[K041.txt

ESET Smart Security 3.0.667.0 - Privilege Escalation (PoC)
| windows/dos/6[01;31m[K25[m[K1.txt

ESET Smart Security 4.2 and NOD32 AntiVirus 4.2 (x86/x64) - LZH archive
parsing (PoC) | windows/dos/1[01;31m[K25[m[K29.py

Eshopbuilde CMS - SQL Injection
| asp/webapps/10[01;31m[K25[m[K3.txt

eSignal and eSignal Pro 10.6.24[01;31m[K25[m[K.1208 - File Parsing
Buffer Overflow in QUO (Metasploit) |
windows/local/17880.rb

eSignal and eSignal Pro 10.6.24[01;31m[K25[m[K.1208 - Multiple
Vulnerabilities |
windows/dos/17837.txt

ESMI PayPal StoreFront 1.7 - 'pages.php?idpages' SQL Injection
| php/webapps/[01;31m[K25[m[K278.sh

ESMI PayPal StoreFront 1.7 - 'products1.php?id2' SQL Injection
| php/webapps/[01;31m[K25[m[K279.txt

ESMI PayPal StoreFront 1.7 - Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K280.txt

eStore 1.0.1/1.0.2 - 'Settings.inc.php' Full Path Disclosure
| php/webapps/229[01;31m[K25[m[K.txt

```
Eternal Lines Web Server 1.0 - Remote Denial of Service
| multiple/dos/[01;31m[K25[m[K075.pl

Ethereal 0.x - Multiple iSNS / SMB / SNMP Protocol Dissector
Vulnerabilities                                  |
linux/remote/24[01;31m[K25[m[K9.c

ETicket 1.5.5 - 'Open.php' Multiple Cross-Site Scripting
Vulnerabilities                                      |
php/webapps/30[01;31m[K25[m[K3.txt

EType EServ 2.98/2.99/3.0 - Resource Exhaustion (Denial of Service) (1)
| windows/dos/2[01;31m[K25[m[K85.pl

EType EServ 2.98/2.99/3.0 - Resource Exhaustion (Denial of Service) (2)
| windows/dos/2[01;31m[K25[m[K86.c

Eurofull E-Commerce - 'Mensresp.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K078.txt

Everest 5.50.2100 - 'Open File' Denial of Service (PoC)
| windows/dos/48[01;31m[K25[m[K9.py

Evolve Merchant - 'viewcart.asp' SQL Injection
| asp/webapps/290[01;31m[K25[m[K.txt

Exam Reviewer Management System 1.0 - ‘id’ SQL Injection
| php/webapps/507[01;31m[K25[m[K.txt

Executables Created with perl2exe < V30.10C - Arbitrary Code Execution
| multiple/remote/518[01;31m[K25[m[K.txt

Exhibit Engine 1.5 RC 4 - 'photo_comment.php' File Inclusion
| php/webapps/[01;31m[K25[m[K09.txt

Exim - 'sender_address' Remote Code Execution
| linux/remote/[01;31m[K25[m[K970.py

Exim 4.63 - Remote Command Execution
| linux/remote/157[01;31m[K25[m[K.pl

Exim4 < 4.69 - string_format Function Heap Buffer Overflow (Metasploit)
| linux/remote/169[01;31m[K25[m[K.rb

EXoops - Multiple Input Validation Vulnerabilities
| php/webapps/[01;31m[K25[m[K300.txt

Exponent CMS 0.95 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K058.txt

Exponent CMS 2.2.0 Beta 3 - Multiple Vulnerabilities
| php/webapps/[01;31m[K25[m[K518.txt
```

```
Extract Website - 'Filename' File Disclosure
| php/webapps/75[01;31m[K25[m[K.txt

Extrakt Framework 0.7 - 'index.php' Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K47.txt

eXV2 Module eblog 1.2 - 'blog_id' SQL Injection
| php/webapps/5[01;31m[K25[m[K3.txt

eXV2 Module MyAnnonces - 'lid' SQL Injection
| php/webapps/5[01;31m[K25[m[K2.txt

eXV2 Module Viso 2.0.4.3 - 'kid' SQL Injection
| php/webapps/5[01;31m[K25[m[K4.txt

eXV2 Module WebChat 1.60 - 'roomid' SQL Injection
| php/webapps/5[01;31m[K25[m[K5.txt

EyesOfNetwork 5.3 - Remote Code Execution
| php/webapps/480[01;31m[K25[m[K.txt

EZ Server 1.0 - File Disclosure
| windows/remote/2[01;31m[K25[m[K06.txt

f-fileman 7.0 - Directory Traversal
| cgi/webapps/17[01;31m[K25[m[K9.txt

F-PROT AntiVirus 6.2.1.4[01;31m[K25[m[K2 - Malformed Archive Infinite
Loop Denial of Service                                |
multiple/dos/6174.txt

F3Site 2.1 - Remote Code Execution
| php/webapps/3[01;31m[K25[m[K5.php

Factux - Local File Inclusion
| php/webapps/1[01;31m[K25[m[K21.txt

family connections 2.2.3 - Multiple Vulnerabilities
| php/webapps/1[01;31m[K25[m[K57.txt

Fast Free Media 1.3 Adult Site - Arbitrary File Upload
| php/webapps/1[01;31m[K25[m[K69.html

Fastpublish CMS 1.9999 - config[fsBase] Remote File Inclusion
| php/webapps/47[01;31m[K25[m[K.txt

Fastream NETFile FTP/Web Server 6.5/6.7 - Directory Traversal
| cgi/webapps/24[01;31m[K25[m[K2.txt

FastStone 4in1 Browser 1.2 - Web Server Directory Traversal
| windows/remote/[01;31m[K25[m[K319.txt
```

```
FCKEditor Core - 'FileManager test.html' Arbitrary File Upload (1)
| php/webapps/12[01;31m[K25[m[K4.txt

FiberHome ADSL AN1020-[01;31m[K25[m[K - Improper Access Restrictions
| hardware/webapps/42649.txt

File 3.x - Local Stack Overflow Code Execution (2)
| unix/local/223[01;31m[K25[m[K.c

File Lite 3.3/3.5 PRO iOS - Multiple Vulnerabilities
| ios/webapps/[01;31m[K25[m[K417.txt

FileOptimizer 14.00.[01;31m[K25[m[K24 - Denial of Service (PoC)
| windows/dos/47586.py

Finjan SurfinGate 7.0 - '.ASCII' File Extension File Filter
Circumvention                                    |
linux/remote/[01;31m[K25[m[K820.txt

Fiomental & Coolsis Backoffice - Multiple Vulnerabilities
| php/webapps/1[01;31m[K25[m[K63.txt

FipsCMS 2.1 - 'neu.asp' SQL Injection
| asp/webapps/32[01;31m[K25[m[K5.txt

Firebird 1.0 - GDS_Inet_Server Interbase Environment Variable Buffer
Overflow                                  |
freebsd/local/2[01;31m[K25[m[K80.c

Firefly Studios Stronghold 2 - Remote Denial of Service
| multiple/dos/[01;31m[K25[m[K757.txt

Firefox 55.0.3 - Denial of Service (PoC)
| windows_x86-64/dos/45[01;31m[K25[m[K7.txt

firmCHANNEL Indoor & Outdoor Digital Signage 3.24 - Cross-Site
Scripting                                        |
php/webapps/3[01;31m[K25[m[K66.txt

FishCart 3.1 - 'display.php?nlst' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K601.txt

FishCart 3.1 - 'display.php?psku' SQL Injection
| php/webapps/[01;31m[K25[m[K603.txt

FishCart 3.1 - 'upstnt.php?cartid' SQL Injection
| php/webapps/[01;31m[K25[m[K604.txt

FishCart 3.1 - 'upstracking.php' Multiple Cross-Site Scripting
Vulnerabilities                                  |
php/webapps/[01;31m[K25[m[K602.txt
```

```
Fitnesse Wiki - Remote Command Execution (Metasploit)
| windows/remote/3[01;31m[K25[m[K68.rb

FiverrScript - Cross-Site Request Forgery (Add Admin)
| php/webapps/37[01;31m[K25[m[K7.txt

Flash Poker 2.0 - 'game' SQL Injection
| php/webapps/4[01;31m[K25[m[K74.txt

FlashFXP 1.4 - User Password Encryption
| windows/local/2[01;31m[K25[m[K64.c

FlashGet 1.9.0.1012 - 'FTP PWD Response' Remote Buffer Overflow
(SafeSEH)                                    |
windows/remote/6[01;31m[K25[m[K6.pl

FlatNuke 2.5.x - 'help.php' Multiple Cross-Site Scripting
Vulnerabilities                                  |
php/webapps/[01;31m[K25[m[K800.txt

FlatNuke 2.5.x - 'index.php?where' Full Path Disclosure
| php/webapps/[01;31m[K25[m[K799.txt

FlatNuke 2.5.x - 'referer.php' Crafted Referer Arbitrary PHP Code
Execution                                   |
php/webapps/[01;31m[K25[m[K801.php

flatnux 2021-03.[01;31m[K25[m[K - Remote Code Execution (Authenticated)
| php/webapps/51295.txt

FlexCMS 2.5 - 'inc-core-admin-editor-previouscolorsjs.php' Cross-Site
Scripting                              |
php/webapps/32[01;31m[K25[m[K4.txt

Flipper Poll 1.1.0 - 'poll.php?root_path' Remote File Inclusion
| php/webapps/3[01;31m[K25[m[K3.txt

FloosieTek FTGate PRO 1.22 - SMTP MAIL FROM Buffer Overflow
| windows/dos/2[01;31m[K25[m[K68.pl

FloosieTek FTGate PRO 1.22 - SMTP RCPT TO Buffer Overflow
| windows/dos/2[01;31m[K25[m[K69.pl

Flussonic Media Server 4.1.[01;31m[K25[m[K < 4.3.3 - Arbitrary File
Disclosure                                              | aix/dos/33943.txt

Foafgen 0.3 - 'redir.php' Local Source Disclosure
| php/webapps/[01;31m[K25[m[K06.txt

Foe CMS 1.6.5 - Multiple Vulnerabilities
| php/webapps/[01;31m[K25[m[K088.txt
```

```
Fool's Workshop Owl's Workshop 1.0 - '/glossaries/index.php?File'
Arbitrary File Access                    |
php/webapps/237[01;31m[K25[m[K.txt

Foxit PDF Reader 1.0.1.09[01;31m[K25[m[K -
CFX_BaseSegmentedArray::IterateIndex Memory Corruption
| linux/dos/39944.txt

Foxit PDF Reader 1.0.1.09[01;31m[K25[m[K - CFX_WideString::operator=
Invalid Read                                          |
linux/dos/39942.txt

Foxit PDF Reader 1.0.1.09[01;31m[K25[m[K -
CPDF_DIBSource::TranslateScanline24bpp Out-of-Bounds Read
| linux/dos/39941.txt

Foxit PDF Reader 1.0.1.09[01;31m[K25[m[K -
CPDF_StreamContentParser::~CPDF_StreamContentParser Heap Memory
Corruption   | linux/dos/39940.txt

Foxit PDF Reader 1.0.1.09[01;31m[K25[m[K -
kdu_core::kdu_codestream::get_subsampling Memory Corruption
| linux/dos/39943.txt

Foxit Reader 3.1.4.11[01;31m[K25[m[K - ActiveX Heap Overflow (PoC)
| windows/dos/11196.html

Free Advertisment CMS - 'user_info.php' SQL Injection
| php/webapps/1[01;31m[K25[m[K72.txt

Free Mp3 Player 1.0 - Local Denial of Service
| windows/dos/18[01;31m[K25[m[K4.pl

FreeBSD 5.4/6.0 - 'ptrace PT_LWPINFO' Local Denial of Service
| bsd/dos/[01;31m[K25[m[K24.c

FreeBSD 6.1-RELEASE-p10 - 'ftruncate' Local Denial of Service
| bsd/dos/[01;31m[K25[m[K41.c

FreeBSD 6.1-RELEASE-p10 - 'scheduler' Local Denial of Service
| bsd/dos/[01;31m[K25[m[K42.c

FreeBSD 7.x - Dumping Environment Local Kernel Panic (Denial of
Service)                                    |
freebsd/dos/8[01;31m[K25[m[K9.c

FreeBSD 8.0 Run-Time Link-Editor (RTLD) - Local Privilege Escalation
| bsd/local/10[01;31m[K25[m[K5.txt

FreePBX - 'config.php' Remote Code Execution (Metasploit)
| unix/remote/3[01;31m[K25[m[K12.rb
```

```
Freeway 1.4.1.171 - '/english/account.php?language' Traversal Local
File Inclusion                          |
php/webapps/32[01;31m[K25[m[K9.txt

FreezingCold Broadboard - 'search.asp' SQL Injection
| asp/webapps/246[01;31m[K25[m[K.txt

Froxlor Server Management Panel 0.9.33.1 - MySQL Login Information
Disclosure                              |
php/webapps/377[01;31m[K25[m[K.txt

FS Amazon Clone 1.0 - SQL Injection
| php/webapps/43[01;31m[K25[m[K9.txt

FS Care Clone 1.0 - 'jobFrequency' / 'jobType' SQL Injection
| php/webapps/43[01;31m[K25[m[K8.txt

FS Crowdfunding Script 1.0 - 'latest_news_details.php?id' SQL Injection
| php/webapps/43[01;31m[K25[m[K7.txt

FS Ebay Clone 1.0 - 'id' / 'sub_category_id' / 'category_id' SQL
Injection                                |
php/webapps/43[01;31m[K25[m[K6.txt

FS Freelancer Clone 1.0 - 'profile.php?u' SQL Injection
| php/webapps/43[01;31m[K25[m[K5.txt

FS Gigs Script 1.0 - 'cat' / 'sc' SQL Injection
| php/webapps/43[01;31m[K25[m[K4.txt

FS Groupon Clone 1.0 - 'id' SQL Injection
| php/webapps/43[01;31m[K25[m[K3.txt

FS Grubhub Clone 1.0 - 'keywords' SQL Injection
| php/webapps/43[01;31m[K25[m[K2.html

FS IMDB Clone 1.0 - 'f' / 's' / 'id' SQL Injection
| php/webapps/43[01;31m[K25[m[K1.txt

FS Indiamart Clone 1.0 - 'token' / 'id' / 'c' SQL Injection
| php/webapps/43[01;31m[K25[m[K0.txt

fsboard 2.0 - Directory Traversal
| asp/webapps/[01;31m[K25[m[K924.txt

FTP Drive + HTTP 1.0.4 iOS - Code Execution
| ios/webapps/3[01;31m[K25[m[K57.txt

FTP Made Easy PRO 1.2 - SQL Injection
| php/webapps/4[01;31m[K25[m[K70.txt
```

FTPGetter Standard 3.55.0.05 - Remote Stack Buffer Overflow (PWD) (Metasploit) |
windows/remote/167[01;31m[K25[m[K.rb

FUN labs Game Engine - Multiple Remote Denial of Service Vulnerabilities |
windows/dos/[01;31m[K25[m[K[01;31m[K25[m[K5.txt

FunkyASP AD Systems 1.1 - 'login.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K705.txt

Funny Image and Video Script 2.0.0 - 'id' SQL Injection
| php/webapps/41[01;31m[K25[m[K8.txt

FUSE 2.2/2.3 - Local Information Disclosure
| linux/local/[01;31m[K25[m[K789.c

FusionBB 0.x - Multiple Input Validation Vulnerabilities
| php/webapps/[01;31m[K25[m[K819.txt

Fusionphp Fusion News 3.3/3.6 - X-Forworded-For PHP Script Code Injection |
php/webapps/[01;31m[K25[m[K681.php

FuzeZip 1.0.0.1316[01;31m[K25[m[K - Local Buffer Overflow (SEH)
| windows/local/[01;31m[K25[m[K130.py

G DATA Total Security [01;31m[K25[m[K.4.0.3 - Activex Buffer Overflow |
windows/dos/45017.html

Gadu-Gadu 6.0 - URL Parser JavaScript Cross-Site Scripting
| windows/remote/[01;31m[K25[m[K009.txt

Gaim 1.1.3 - File Download Denial of Service
| linux/dos/[01;31m[K25[m[K164.txt

Galeria Zdjec 3.0 - 'zd_numer.php' Local File Inclusion
| php/webapps/32[01;31m[K25[m[K.pl

Garment Center - 'index.cgi' Local File Inclusion
| cgi/webapps/310[01;31m[K25[m[K.txt

Gazelle CMS 1.0 - Multiple Vulnerabilities / Remote Code Execution
| php/webapps/94[01;31m[K25[m[K.sh

GD Graphics Library 2.0.34 - 'libgd' gdImageCreateXbm Function Unspecified Denial of Service |
linux/dos/30[01;31m[K25[m[K1.c

Gearbox Software Halo Game Server 1.06/1.07 - Infinite Loop Denial of Service |
windows/dos/[01;31m[K25[m[K699.txt

```
Gedit 2.x - Filename Format String
| linux/local/[01;31m[K25[m[K688.txt

Geeklog 1.3.5 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/215[01;31m[K25[m[K.txt

Gemtek CPE7000 - WLTCS-106 Administrator SID Retriever (Metasploit)
| hardware/webapps/397[01;31m[K25[m[K.rb

Genepi 1.6 - 'genepi.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K39.txt

Gentoo Webapp-Config 1.10 - Insecure File Creation
| linux/local/[01;31m[K25[m[K709.sh

Geodesic Solutions (Multiple Products) - 'index.php?b' SQL Injection
| php/webapps/28[01;31m[K25[m[K0.txt

GeoHttpServer - Remote Denial of Service
| windows/dos/1[01;31m[K25[m[K31.pl

GeoVision (GeoHttpServer) Webcams - Remote File Disclosure
| hardware/webapps/37[01;31m[K25[m[K8.py

GeoVision Digital Surveillance System 6.0 4/6.1 - Unauthorized '.JPEG'
Image Access                          |
windows/remote/[01;31m[K25[m[K643.txt

GeSHi 1.0.x - XML Parsing Remote Denial of Service
| multiple/dos/3[01;31m[K25[m[K96.txt

Getsimple CMS 2.01 - Local File Inclusion
| php/webapps/1[01;31m[K25[m[K17.txt

Getsimple CMS 3.2.1 - Arbitrary File Upload
| php/webapps/[01;31m[K25[m[K405.txt

Getsimple CMS 3.3.1 - Persistent Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K02.txt

Geutebruck 5.02024 G-Cam/EFD-2[01;31m[K25[m[K0 - 'simple_loglistjs.cgi'
Remote Command Execution (Metasploit)           |
hardware/webapps/44957.rb

Geutebruck 5.02024 G-Cam/EFD-2[01;31m[K25[m[K0 - 'testaction.cgi'
Remote Command Execution (Metasploit)                 |
hardware/webapps/41360.rb

GForge 3.x - Arbitrary Command Execution
| php/webapps/[01;31m[K25[m[K693.txt

Git < 2.7.5 - Command Injection (Metasploit)
| python/remote/4[01;31m[K25[m[K99.rb
```

```
GitLab 11.4.7 - Remote Code Execution (Authenticated) (1)
| ruby/webapps/49[01;31m[K25[m[K7.py

GlassFish Application Server - '/resourceNode/jmsConnectionNew.jsf'
Multiple Cross-Site Scripting Vulnerab |
multiple/remote/319[01;31m[K25[m[K.txt

Gleez CMS 1.2.0 - Cross-Site Request Forgery (Add Admin)
| php/webapps/45[01;31m[K25[m[K8.txt

glFTPd 1.x/2.0 'ZIP' Plugins - Multiple Directory Traversal
Vulnerabilities                                  |
linux/remote/[01;31m[K25[m[K122.txt

glibc - 'LD_AUDIT' Arbitrary DSO Load Privilege Escalation (Metasploit)
| linux/local/440[01;31m[K25[m[K.rb

glibc-2.2 / openssh-2.3.0p1 / glibc 2.1.9x - File Read
| linux/local/[01;31m[K25[m[K8.sh

GlobalNoteScript 4.20 - 'Read.cgi' Remote Command Execution
| cgi/webapps/[01;31m[K25[m[K939.txt

GNU GNATS 4.0/4.1 - Gen-Index Arbitrary Local File Disclosure/Overwrite
| linux/local/[01;31m[K25[m[K947.txt

GNU Mailutils 0.6 - Mail Email Header Buffer Overflow
| linux/remote/[01;31m[K25[m[K706.cpp

GNU screen v4.9.0 - Privilege Escalation
| linux/local/51[01;31m[K25[m[K2.py

GNU UnRTF 0.19.3 - Font Table Conversion Buffer Overflow
| linux/remote/[01;31m[K25[m[K030.txt

GnuPG 1.4/1.9 - Parse_Comment Remote Buffer Overflow
| linux/dos/28[01;31m[K25[m[K7.txt

Golden FTP Server 4.30 - File Deletion
| windows/remote/10[01;31m[K25[m[K8.pl

GoldLink 3.0 - Cookie SQL Injection
| php/webapps/23[01;31m[K25[m[K9.txt

GoodiWare GoodReader iPhone - '.XLS' Denial of Service
| hardware/dos/138[01;31m[K25[m[K.txt

Google Chrome (Fedora [01;31m[K25[m[K / Ubuntu 16.04) - 'tracker-
extract' / 'gnome-video-thumbnailer' + 'totem' Drive-B |
linux/local/40943.txt

Google Chrome - Denial of Service
| multiple/dos/180[01;31m[K25[m[K.txt
```

```
Google Chrome 72.0.3626.121 / 74.0.37[01;31m[K25[m[K.0 -
'NewFixedDoubleArray' Integer Overflow                          |
multiple/remote/46748.txt

Gossamer Threads Links 2.x - 'User.cgi' Cross-Site Scripting
| cgi/webapps/[01;31m[K25[m[K594.txt

GrayCMS 1.1 - 'error.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K538.txt

GREED 0.81 - '.GRX' File List Buffer Overflow
| windows/remote/[01;31m[K25[m[K033.txt

GREED 0.81 - '.GRX' File List Command Execution
| windows/remote/[01;31m[K25[m[K034.txt

Green Shop - SQL Injection
| php/webapps/14[01;31m[K25[m[K9.txt

GreenCMS 2.3.0603 - Cross-Site Request Forgery / Remote Code Execution
| php/webapps/448[01;31m[K25[m[K.html

Gretech GOM Encoder 1.0.0.11 - '.Subtitle' Buffer Overflow (PoC)
| windows/dos/82[01;31m[K25[m[K.py

GroundWork - 'monarch_scan.cgi' OS Command Injection (Metasploit)
| linux/remote/[01;31m[K25[m[K001.rb

GSM SIM Utility 5.15 - Direct RET Overflow
| windows/local/14[01;31m[K25[m[K8.py

GuppY 4.6.14 - 'lng' Multiple SQL Injections
| php/webapps/355[01;31m[K25[m[K.txt

Guru JustAnswer Professional 1.[01;31m[K25[m[K - Multiple SQL
Injections                                                      |
php/webapps/17350.txt

H&H Solutions WebSoccer 2.80 - 'id' SQL Injection
| php/webapps/3[01;31m[K25[m[K41.txt

H2O-CMS 3.4 - PHP Code Injection / Cookie Authentication Bypass
| php/webapps/3[01;31m[K25[m[K40.pl

h5ai < 0.[01;31m[K25[m[K.0 - Unrestricted Arbitrary File Upload
| php/webapps/38[01;31m[K25[m[K6.py

Hadoop YARN ResourceManager - Command Execution (Metasploit)
| linux/remote/450[01;31m[K25[m[K.rb

Haihaisoft HUPlayer 1.0.4.8 - '.m3u' / '.pls' / '.asx' Buffer Overflow
(SEH)                                | windows/dos/3[01;31m[K25[m[K13.py
```

Haihaisoft Universal Player 1.5.8 - '.m3u' / '.pls '/ '.asx' Buffer Overflow (SEH) |
windows/dos/3[01;31m[K25[m[K14.py

HappyMall E-Commerce Software 4.3/4.4 - 'Member_HTML.cgi' Command Execution |
cgi/webapps/2[01;31m[K25[m[K72.pl

HappyMall E-Commerce Software 4.3/4.4 - 'Normal_HTML.cgi' Command Execution |
cgi/webapps/2[01;31m[K25[m[K71.pl

Happymall E-Commerce Software 4.3/4.4 - 'Normal_HTML.cgi' Cross-Site Scripting |
cgi/webapps/2[01;31m[K25[m[K88.txt

Happymall E-Commerce Software 4.3/4.4 - 'Normal_HTML.cgi' File Disclosure |
cgi/webapps/2[01;31m[K25[m[K92.txt

Harris WapChat 1 - Multiple Remote File Inclusions
| php/webapps/55[01;31m[K25[m[K.txt

Heaven Soft CMS 4.7 - SQL Injection
| php/webapps/1[01;31m[K25[m[K99.txt

HelpCenter Live! 1.0/1.2.x - Multiple Input Validation Vulnerabilities
| php/webapps/[01;31m[K25[m[K683.txt

Hero DVD Remote 1.0 - Remote Buffer Overflow
| windows/remote/14[01;31m[K25[m[K7.py

Hitachi NAS (HNAS) System Management Unit (SMU) Backup & Restore < 14.8.78[01;31m[K25[m[K.01 - IDOR |
hardware/webapps/51872.py

HNAS SMU 14.8.78[01;31m[K25[m[K - Information Disclosure
| hardware/remote/51915.py

HNB 1.9.18-10 - Local Buffer Overflow
| linux/local/400[01;31m[K25[m[K.py

HolaCMS 1.2.x/1.4.x Voting Module - Directory Traversal Remote File Corruption |
php/webapps/[01;31m[K25[m[K222.html

HolaCMS 1.2/1.4.x Voting Module - Remote File Corruption
| php/webapps/[01;31m[K25[m[K217.html

Home FTP Server 1.12 - Directory Traversal
| windows/remote/16[01;31m[K25[m[K9.txt

Home of Viral Images_ Videos and Articles Script - SQL Injection
| php/webapps/411[01;31m[K25[m[K.txt

Hornbill Supportworks ITSM 1.0.0 - SQL Injection
| php/webapps/[01;31m[K25[m[K002.txt

Hosting Controller 1.x/6.1 - Multiple Information Disclosure
Vulnerabilities |
windows/remote/[01;31m[K25[m[K194.txt

Hosting Controller 6.1 - 'error.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K913.txt

Hosting Controller 6.1 - 'plandetails.asp' Information Disclosure
| asp/webapps/[01;31m[K25[m[K754.txt

Hosting Controller 6.1 - 'resellerresources.asp?jresourceid' SQL
Injection |
asp/webapps/[01;31m[K25[m[K753.txt

Hosting Controller 6.1 - Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K981.txt

Hosting Controller 6.1 - User Profile Unauthorized Access
| asp/webapps/[01;31m[K25[m[K758.txt

Hotel and Lodge Management System 1.0 - Remote Code Execution
(Unauthenticated) |
php/webapps/496[01;31m[K25[m[K.py

HP Color LaserJet [01;31m[K25[m[K00/4600 Toolbox - Directory Traversal
| windows/remote/27565.txt

HP Instant Support - ActiveX Control Driver Check Buffer Overflow
| windows/remote/30[01;31m[K25[m[K7.html

HP LaserJet Pro P1606dn - Webadmin Password Reset
| hardware/webapps/[01;31m[K25[m[K715.py

HP OfficeJet 4630/7110 MYM1FN20[01;31m[K25[m[KAR/2117A - Stored Cross-
Site Scripting (XSS) |
hardware/webapps/50227.py

HP OpenView Network Node Manager (OV NNM) 7.53 - 'ovwebsnmpsrv.exe'
Local Buffer Overflow (SEH) |
windows/local/14[01;31m[K25[m[K6.txt

HP OpenView Radia 2.0/3.1/4.0 - Notify Daemon Multiple Remote Buffer
Overflow Vulnerabilities |
windows/dos/[01;31m[K25[m[K782.txt

HP OpenView Radia Management Portal 1.0/2.0 - Remote Command Execution
| windows/remote/[01;31m[K25[m[K557.txt

HP WebInspect 10.4 - XML External Entity Injection
| xml/webapps/37[01;31m[K25[m[K0.txt

HP-UX 10.x/11.x - RExec Remote 'Username' Flag Local Buffer Overrun
| hp-ux/dos/2[01;31m[K25[m[K52.txt

HP-UX 10/11/ IRIX 3/4/5/6 / OpenSolaris build snv / Solaris 8/9/10 /
SunOS 4.1 - 'rpc.ypupdated' Command E |
multiple/remote/20[01;31m[K25[m[K8.c

HP-UX 10/11/ IRIX 3/4/5/6 / OpenSolaris build snv / Solaris 8/9/10 /
SunOS 4.1 - 'rpc.ypupdated' Command E |
multiple/remote/20[01;31m[K25[m[K9.txt

HP-UX 11 RWrite - Buffer Overflow
| hp-ux/dos/2[01;31m[K25[m[K61.txt

HP-UX FTP Server - Directory Listing (Metasploit)
| hp-ux/remote/1[01;31m[K25[m[K9.pm

HTC Touch - vCard over IP Denial of Service
| hardware/dos/81[01;31m[K25[m[K.py

HTML2HDML 1.0.3 - File Conversion Buffer Overflow
| multiple/remote/[01;31m[K25[m[K011.txt

Huawei HG[01;31m[K25[m[K5 - Directory Traversal (Metasploit)
| hardware/webapps/47923.rb

Huawei HG[01;31m[K25[m[K5s - Directory Traversal
| hardware/webapps/42634.txt

Huawei Home Gateway UPnP/1.0 IGD/1.00 - Password Change
| hardware/webapps/374[01;31m[K25[m[K.py

Huawei SNMPv3 Service - Multiple Buffer Overflow Vulnerabilities (PoC)
| hardware/dos/[01;31m[K25[m[K295.txt

Human Resource Management System 1.0 - SQL Injection (unauthenticated)
| php/webapps/511[01;31m[K25[m[K.txt

Hunk Companion Plugin 1.9.0 - Unauthenticated Plugin Installation
| multiple/webapps/52[01;31m[K25[m[K9.py

Hyplay 1.2.326.1 - '.asx' Local Denial of Service Crash (PoC)
| windows/dos/1[01;31m[K25[m[K46.pl

I-Gallery - Folder Argument Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K855.txt

I-Gallery - Folder Argument Directory Traversal
| asp/webapps/[01;31m[K25[m[K853.txt

```
i-Net Solution Matrimonial Script 2.0.3 - 'alert.php' Cross-Site
Scripting                                  |
php/webapps/34[01;31m[K25[m[K2.txt

Iatek IntranetApp 2.3 - 'ad_click.asp?banner_id' SQL Injection
| asp/webapps/[01;31m[K25[m[K318.txt

iBall Baton 150M Wireless Router - Authentication Bypass
| php/webapps/4[01;31m[K25[m[K91.txt

IBM AIX 5.x - 'Diag' Local Privilege Escalation
| aix/local/[01;31m[K25[m[K039.txt

IBM AIX 5.x - 'Invscout' Local Buffer Overflow
| aix/dos/[01;31m[K25[m[K807.txt

IBM AIX 6.1.8 - 'libodm' Arbitrary File Write
| aix/local/337[01;31m[K25[m[K.txt

IBM Bladecenter Management Module - Denial of Service
| hardware/dos/12[01;31m[K25[m[K2.txt

IBM Cognos Business Intelligence - XML External Entity Information
Disclosure                                 |
multiple/remote/388[01;31m[K25[m[K.xml

IBM GCM16/32 1.20.0.2[01;31m[K25[m[K75 - Multiple Vulnerabilities
| php/remote/34132.txt

IBM Informix SE 7.[01;31m[K25[m[K sqlexec - Local Buffer Overflow (1)
| linux/local/21496.c

IBM Informix SE 7.[01;31m[K25[m[K sqlexec - Local Buffer Overflow (2)
| linux/local/21497.pl

IBM iSeries AS400 LDAP Server - Remote Information Disclosure
| unix/remote/[01;31m[K25[m[K335.txt

IBM Lotus Connections 2.0.1 - 'simpleSearch.do' Cross-Site Scripting
| java/webapps/33[01;31m[K25[m[K4.txt

IBM Lotus Domino Notes 6.0/6.5 - Mail Template Automatic Script
Execution                                  |
multiple/remote/[01;31m[K25[m[K944.txt

IBM Lotus Domino Server 6.5.1 Web Service - Remote Denial of Service
| unix/dos/[01;31m[K25[m[K353.txt

IBM OpenAdmin Tool - SOAP welcomeServer PHP Code Execution (Metasploit)
| php/remote/4[01;31m[K25[m[K41.rb

IBM SPSS SamplePower C1Tab - ActiveX Heap Overflow (Metasploit)
| windows/remote/[01;31m[K25[m[K814.rb
```

```
IBM Tealeaf CX 8.8 - Remote OS Command Injection
| php/webapps/3[01;31m[K25[m[K46.py

IBM Tivoli Netcool Service Quality Manager - Cross-Site Scripting /
HTML Injection                          |
multiple/webapps/3[01;31m[K25[m[K76.txt

IBM Websphere 5.0/5.1/6.0 - Application Server Web Server Root JSP
Source Code Disclosure                  |
multiple/remote/[01;31m[K25[m[K420.txt

Icecast 2.x - XSL Parser Multiple Vulnerabilities
| multiple/remote/[01;31m[K25[m[K238.txt

IceWarp Web Mail 5.3 - 'accountsettings_add.html?accountid' Cross-Site
Scripting                               |
php/webapps/[01;31m[K25[m[K069.txt

IceWarp Web Mail 5.3 - login.html 'Username' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K068.txt

ID Team ID Board 1.1.3 - 'SQL.CLS.php' SQL Injection
| php/webapps/[01;31m[K25[m[K958.txt

IDEAL Migration 4.5.1 - Local Buffer Overflow (Metasploit)
| windows/local/1[01;31m[K25[m[K40.rb

IDT PC Audio 1.0.64[01;31m[K25[m[K.0 - 'STacSV' Unquoted Service Path
| windows/local/49043.txt

iGeneric iG Shop 1.x - Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K149.txt

IKE - Aggressive Mode Shared Secret Hash Leakage
| hardware/remote/2[01;31m[K25[m[K32.txt

IkonBoard 3.1 - Lang Cookie Arbitrary Command Execution (2)
| cgi/webapps/2[01;31m[K25[m[K00.pl

ilchClan 1.0.5B - SQL Injection
| php/webapps/12[01;31m[K25[m[K6.txt

ImageMagick 6.x - '.PNM' Image Decoding Remote Buffer Overflow
| linux/dos/[01;31m[K25[m[K527.txt

ImageMagick 7.1.0-49 - DoS
| php/dos/51[01;31m[K25[m[K6.txt

IMAP4rev1 10.190 - Authentication Stack Overflow
| linux/remote/[01;31m[K25[m[K3.pl

iMLog < 1.307 - Persistent Cross Site Scripting (XSS)
| php/webapps/520[01;31m[K25[m[K.txt
```

```
Imperva SecureSphere Operations Manager 9.0.0.5 - Multiple
Vulnerabilities                                    |
jsp/webapps/[01;31m[K25[m[K977.txt

IncCMS Core 1.0.0 - 'settings.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K57.txt

IndexScript 2.8 - 'cat_id' SQL Injection
| php/webapps/42[01;31m[K25[m[K.txt

Indexu 5.0 - Multiple Remote File Inclusions
| php/webapps/276[01;31m[K25[m[K.txt

Indexu 5.0.1 - 'admin_template_path' Remote File Inclusion
| php/webapps/19[01;31m[K25[m[K.txt

India Software Solution Shopping Cart - SQL Injection
| php/webapps/[01;31m[K25[m[K756.txt

Info-ZIP UnZip 5.50 - Encoded Character Hostile Destination Path
| linux/remote/2[01;31m[K25[m[K84.txt

Infoproject Business Hero - Multiple Vulnerabilities
| php/webapps/18[01;31m[K25[m[K9.txt

Integramod Portal 2.0 rc2 - 'phpbb_root_path' Remote File Inclusion
| php/webapps/2[01;31m[K25[m[K6.txt

Integramod Portal 2.x - 'functions_portal.php' Remote File Inclusion
| php/webapps/2[01;31m[K25[m[K0.pl

Integrated CMS 1.0 - SQL Injection
| php/webapps/275[01;31m[K25[m[K.txt

Interactive Studio GamePort 3.0/3.1/4.0 - Arbitrary Application
Execution                                          |
windows/remote/[01;31m[K25[m[K013.txt

InterAKT Online MX Shop 1.1.1 - SQL Injection
| php/webapps/[01;31m[K25[m[K323.txt

Internet Download Manager 6.[01;31m[K25[m[K Build 14 - 'Find file'
Unicode (SEH)                                      |
windows/local/39579.py

Interspire articlelive 2005 - Multiple Vulnerabilities
| php/webapps/[01;31m[K25[m[K599.txt

Interspire ArticleLive 2005 - NewComment Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K262.txt

InterWorx Control Panel 5.0.13 build 574 - 'xhr.php?i' SQL Injection
| php/webapps/3[01;31m[K25[m[K16.txt
```

```
Intrasrv Simple Web Server 1.0 - Remote Code Execution (SEH)
| windows/remote/[01;31m[K25[m[K836.py

InverseFlow 2.4 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/36[01;31m[K25[m[K3.txt

Invision Community Blog 1.0/1.1 - Multiple Input Validation
Vulnerabilities                                  |
php/webapps/[01;31m[K25[m[K808.txt

Invision Gallery 2.0.7 (Linux) - 'readfile()' / SQL Injection
| php/webapps/[01;31m[K25[m[K27.c

Invision Power Board (IP.Board) 1.x/2.0.3 - SML Code Script Injection
| php/webapps/[01;31m[K25[m[K143.txt

Invision Power Board (IP.Board) 2.0.3/2.1 - 'Act' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K593.txt

Invision Power Board (IP.Board) 2.3.5 - Multiple Vulnerabilities (2)
| php/webapps/63[01;31m[K25[m[K.php

Invision Power Board (IP.Board) 3.3.4 - Unserialize Regex Bypass
| php/webapps/2[01;31m[K25[m[K47.php

Invision Power Board 1.x - 'ST' SQL Injection
| php/webapps/[01;31m[K25[m[K380.txt

Invision Power Board 1.x - Unauthorized Access
| php/webapps/[01;31m[K25[m[K741.bat

Invision Power Board 1.x/2.0 - HTML Injection
| php/webapps/[01;31m[K25[m[K267.txt

Invision Power Board 1.x?/2.x/3.x - Admin Takeover
| php/webapps/[01;31m[K25[m[K441.txt

Invision Power Board 2.0.1 - 'QPid' SQL Injection
| php/webapps/[01;31m[K25[m[K535.txt

Invision Power Board 3.0.1 - SQL Injection
| php/webapps/1[01;31m[K25[m[K86.php

Invision Power Services Invision Gallery 1.0.1/1.3 - SQL Injection
| php/webapps/[01;31m[K25[m[K806.txt

Invoice Manager 3.1 - Cross-Site Request Forgery (Add Admin)
| php/webapps/4[01;31m[K25[m[K92.html

IObit Malware Fighter 4.3.1 - Unquoted Service Path Privilege
Escalation                                       |
windows/local/405[01;31m[K25[m[K.txt
```

```
iParty Conferencing Server - Denial of Service
| multiple/dos/22[01;31m[K25[m[K0.sh

iPeGuestbook 1.7/2.0 - 'pg' Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K28.txt

IPFire 2.[01;31m[K25[m[K - Remote Code Execution (Authenticated)
| cgi/webapps/49869.py

Ipswitch IMail 11.01 - Cross-Site Scripting
| windows/webapps/[01;31m[K25[m[K086.pl

Ipswitch WhatsUp Professional 2005 SP1 - 'login.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K874.txt

Ipswitch WhatsUp Professional 2006 - Remote Denial of Service
| asp/dos/27[01;31m[K25[m[K8.txt

Ipswitch WS_FTP Home/Professional 8.0 - WS_FTP Client Format String
| windows/dos/32[01;31m[K25[m[K6.py

Ipswitch WS_FTP Home/Professional FTP Client - Remote Format String
(PoC)                                    |
windows/dos/6[01;31m[K25[m[K7.pl

IrfanView - '.tiff' Image Processing Buffer Overflow
| windows/dos/18[01;31m[K25[m[K7.txt

IrfanView FlashPix PlugIn - Double-Free
| windows/dos/18[01;31m[K25[m[K6.txt

iScripts AutoHoster 3.0 - 'siteid' SQL Injection
| php/webapps/41[01;31m[K25[m[K1.txt

iScripts EasyCreate 3.2 - 'siteid' SQL Injection
| php/webapps/41[01;31m[K25[m[K2.txt

iSmartViewPro 1.5 - 'DDNS' Buffer Overflow
| windows_x86/local/453[01;31m[K25[m[K.py

ISPConfig 3.0.5.4p6 - Multiple Vulnerabilities
| php/webapps/37[01;31m[K25[m[K9.txt

iStArtApp FileXChange 6.2 iOS - Multiple Vulnerabilities
| ios/webapps/3[01;31m[K25[m[K69.txt

iTech B2B Script 4.42 - SQL Injection
| php/webapps/4[01;31m[K25[m[K05.txt

iTech Business Networking Script 8.26 - SQL Injection
| php/webapps/4[01;31m[K25[m[K06.txt
```

iTech Caregiver Script 2.71 - SQL Injection
| php/webapps/4[01;31m[K25[m[K07.txt

iTech Classifieds Script 7.41 - SQL Injection
| php/webapps/4[01;31m[K25[m[K08.txt

iTech Dating Script 3.40 - SQL Injection
| php/webapps/4[01;31m[K25[m[K14.txt

iTech Freelancer Script 5.27 - SQL Injection
| php/webapps/4[01;31m[K25[m[K10.txt

iTech Image Sharing Script 4.13 - SQL Injection
| php/webapps/4[01;31m[K25[m[K09.txt

Itech Job Portal Script 9.13 - Multiple Vulnerabilities
| php/webapps/41[01;31m[K25[m[K0.txt

iTech Job Script 9.27 - SQL Injection
| php/webapps/4[01;31m[K25[m[K15.txt

iTech Movie Script 7.51 - SQL Injection
| php/webapps/4[01;31m[K25[m[K16.txt

iTech Multi Vendor Script 6.63 - SQL Injection
| php/webapps/4[01;31m[K25[m[K13.txt

iTech Social Networking Script 3.08 - SQL Injection
| php/webapps/4[01;31m[K25[m[K29.txt

itech TrainSmart r1044 - SQL injection
| php/webapps/51[01;31m[K25[m[K3.txt

iTech Travel Script 9.49 - SQL Injection
| php/webapps/4[01;31m[K25[m[K11.txt

Jaangle 0.98e.971 - Denial of Service
| windows/dos/145[01;31m[K25[m[K.pl

JAD Java Decompiler 1.5.8e - Local Buffer Overflow (NX Enabled)
| linux/local/42[01;31m[K25[m[K5.py

JamMail 1.8 - Jammail.pl Arbitrary Command Execution
| cgi/webapps/[01;31m[K25[m[K817.txt

JASmine 0.0.2 - 'index.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K05.txt

Jason Hines PHPWebLog 0.4/0.5 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K193.txt

Jaws 0.2/0.3 - 'action' Cross-Site Scripting
| php/webapps/24[01;31m[K25[m[K7.txt

```
Jaws 0.2/0.3 - 'gadget' Traversal Arbitrary File Access
| php/webapps/24[01;31m[K25[m[K5.txt

Jaws 0.2/0.3 - Cookie Manipulation Authentication Bypass
| php/webapps/24[01;31m[K25[m[K6.php

Jaws 0.x - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K942.txt

Jaws Glossary 0.4/0.5 - Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K740.txt

jaZip 0.32-2 - Local Buffer Overflow
| linux/local/[01;31m[K25[m[K7.pl

JBoss 3.x/4.0.2 - HTTP Request Remote Information Disclosure
| multiple/remote/[01;31m[K25[m[K842.txt

JE Ajax Event Calendar - Local File Inclusion
| php/webapps/1[01;31m[K25[m[K98.txt

Jedox 2020.2.5 - Stored Cross-Site Scripting in Log-Module
| php/webapps/514[01;31m[K25[m[K.txt

Jef Moine abcm2ps 3.7.20 - '.ABC' File Remote Buffer Overflow
| windows/remote/[01;31m[K25[m[K022.txt

JetAudio Basic 7.5.5.[01;31m[K25[m[K - '.asx' Buffer Overflow (PoC)
| windows/dos/10651.pl

Jetbox CMS 2.1 - 'liste' Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K[01;31m[K25[m[K.txt

JFrog Artifactory < 7.[01;31m[K25[m[K.4 - Blind SQL Injection
| php/webapps/51806.py

JGS-Portal 3.0.1 - 'ID' SQL Injection
| php/webapps/[01;31m[K25[m[K570.txt

JGS-Portal 3.0.1/3.0.2 - 'jgs_portal.php?anzahl_beitraege' SQL
Injection                                    |
php/webapps/[01;31m[K25[m[K674.txt

JGS-Portal 3.0.1/3.0.2 - 'jgs_portal_beitraggraf.php?year' SQL
Injection                                    |
php/webapps/[01;31m[K25[m[K675.txt

JGS-Portal 3.0.1/3.0.2 - 'jgs_portal_mitgraf.php?year' SQL Injection
| php/webapps/[01;31m[K25[m[K678.txt

JGS-Portal 3.0.1/3.0.2 - 'jgs_portal_sponsor.php?id' SQL Injection
| php/webapps/[01;31m[K25[m[K679.txt
```

JGS-Portal 3.0.1/3.0.2 - 'jgs_portal_statistik.php?year' SQL Injection
| php/webapps/[01;31m[K25[m[K673.txt

JGS-Portal 3.0.1/3.0.2 - 'jgs_portal_themengraf.php?year' SQL Injection
| php/webapps/[01;31m[K25[m[K677.txt

JGS-Portal 3.0.1/3.0.2 - 'jgs_portal_viewsgraf.php?tag' SQL Injection
| php/webapps/[01;31m[K25[m[K676.txt

Jieqi CMS 1.5 - Remote Code Execution
| php/webapps/87[01;31m[K25[m[K.php

Jinzora 2.1 - 'media.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K12.txt

Jinzora 2.6 - '/extras/mt.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K58.txt

JIRA Issues Collector - Directory Traversal (Metasploit)
| windows/remote/327[01;31m[K25[m[K.rb

JiRo's Upload System 1.0 - 'login.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K780.txt

Jive Forums 5.5.[01;31m[K25[m[K - Directory Traversal
| jsp/webapps/39405.py

John Roy Pi3Web 2.0 For Windows - Remote Buffer Overflow
| windows/remote/212[01;31m[K25[m[K.c

Joomla! 3.0.3 - 'remember.php' PHP Object Injection
| php/webapps/[01;31m[K25[m[K087.txt

Joomla! Component aardvertiser 2.0 - Local File Inclusion
| php/webapps/1[01;31m[K25[m[K92.txt

Joomla! Component Advertising 0.[01;31m[K25[m[K - Local File Inclusion
| php/webapps/12171.txt

Joomla! Component Ajax Quiz 1.8 - SQL Injection
| php/webapps/4[01;31m[K25[m[K32.txt

Joomla! Component Almond Classifieds com_aclassf 7.5 - Multiple
Vulnerabilities |
php/webapps/9[01;31m[K25[m[K8.txt

Joomla! Component Article Factory Manager - Arbitrary File Upload
| php/webapps/1[01;31m[K25[m[K39.txt

Joomla! Component Bargain Product VM3 1.0 - 'product_id' SQL Injection
| php/webapps/4[01;31m[K25[m[K52.txt

Joomla! Component Calendar Planner 1.0.1 - SQL Injection
| php/webapps/4[01;31m[K25[m[K01.txt

Joomla! Component Canteen 1.0 - Local File Inclusion
| php/webapps/34[01;31m[K25[m[K0.txt

Joomla! Component com_blog - Directory Traversal
| php/webapps/116[01;31m[K25[m[K.txt

Joomla! Component com_dshop - SQL Injection
| php/webapps/18[01;31m[K25[m[K1.txt

Joomla! Component com_gurujibook - SQL Injection
| php/webapps/112[01;31m[K25[m[K.txt

Joomla! Component com_jeemaarticlecollection - SQL Injection
| php/webapps/106[01;31m[K25[m[K.txt

Joomla! Component com_manager 1.5.3 - 'id' SQL Injection
| php/webapps/12[01;31m[K25[m[K7.txt

Joomla! Component com_org - SQL Injection
| php/webapps/117[01;31m[K25[m[K.txt

Joomla! Component com_PHP 0.1 - Local File Inclusion
| php/webapps/1[01;31m[K25[m[K79.txt

Joomla! Component com_portfolio - Local File Disclosure
| php/webapps/123[01;31m[K25[m[K.txt

Joomla! Component com_s5clanroster - 'id' SQL Injection
| php/webapps/[01;31m[K25[m[K410.txt

Joomla! Component com_sebercart - 'getPic.php' Local File Disclosure
| php/webapps/1[01;31m[K25[m[K94.txt

Joomla! Component com_xmap 1.2.11 - Blind SQL Injection
| php/webapps/175[01;31m[K25[m[K.txt

Joomla! Component Content 1.0.0 - 'itemID' SQL Injection
| php/webapps/60[01;31m[K25[m[K.txt

Joomla! Component dj-classifieds 2.0 - Blind SQL Injection
| php/webapps/[01;31m[K25[m[K248.txt

Joomla! Component FDione Form Wizard 1.0.2 - Local File Inclusion
| php/webapps/1[01;31m[K25[m[K95.txt

Joomla! Component Flip Wall 8.0 - 'wallid' SQL Injection
| php/webapps/4[01;31m[K25[m[K24.txt

Joomla! Component FocalPoint 1.2.3 - SQL Injection
| php/webapps/4[01;31m[K25[m[K30.txt

Joomla! Component Huge-IT Portfolio Gallery Plugin 1.0.6 - SQL Injection |
php/webapps/4[01;31m[K25[m[K97.txt

Joomla! Component Huge-IT Portfolio Gallery Plugin 1.0.7 - SQL Injection |
php/webapps/4[01;31m[K25[m[K98.txt

Joomla! Component Huge-IT Video Gallery 1.0.9 - SQL Injection
| php/webapps/4[01;31m[K25[m[K96.txt

Joomla! Component JD-Wiki 1.0.2 - Remote File Inclusion
| php/webapps/21[01;31m[K25[m[K.txt

Joomla! Component Joomanager 2.0.0 - 'com_Joomanager' Arbitrary File Download |
php/webapps/44[01;31m[K25[m[K2.py

Joomla! Component Joomanager 2.0.0 - 'com_Joomanager' Arbitrary File Download (PoC) |
php/webapps/4[01;31m[K25[m[K90.txt

Joomla! Component Komento 1.0.0 - 'sid' SQL Injection
| php/webapps/1[01;31m[K25[m[K90.txt

Joomla! Component Kunena 3.0.4 - Persistent Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K62.txt

Joomla! Component mod_VisitorData 1.1 - Remote code Execution
| php/webapps/1[01;31m[K25[m[K74.txt

Joomla! Component MusicGallery - SQL Injection
| php/webapps/10[01;31m[K25[m[K0.txt

Joomla! Component NeoRecruit 1.6.4 - 'Itemid' Blind SQL Injection
| php/webapps/14[01;31m[K25[m[K0.txt

Joomla! Component OSDownloads 1.7.4 - SQL Injection
| php/webapps/4[01;31m[K25[m[K61.txt

Joomla! Component Ozio Gallery 2 - Multiple Vulnerabilities
| php/webapps/139[01;31m[K25[m[K.txt

Joomla! Component Permis 1.0 (com_groups) - 'id' SQL Injection
| php/webapps/331[01;31m[K25[m[K.txt

Joomla! Component Photo Contest 1.0.2 - SQL Injection
| php/webapps/4[01;31m[K25[m[K63.txt

Joomla! Component Price Alert 3.0.2 - 'product_id' SQL Injection
| php/webapps/4[01;31m[K25[m[K53.txt

```
Joomla! Component Quick News - SQL Injection
| php/webapps/10[01;31m[K25[m[K2.txt

Joomla! Component Quiz Deluxe 3.7.4 - SQL Injection
| php/webapps/4[01;31m[K25[m[K89.txt

Joomla! Component Realpin 1.5.04 - SQL Injection
| php/webapps/441[01;31m[K25[m[K.txt

Joomla! Component Responsive Portfolio 1.6.1 - SQL Injection
| php/webapps/4[01;31m[K25[m[K64.txt

Joomla! Component SP Movie Database 1.3 - SQL Injection
| php/webapps/4[01;31m[K25[m[K02.txt

Joomla! Component Spider Contacts 1.3.6 - 'contacts_id' SQL Injection
| php/webapps/346[01;31m[K25[m[K.py

Joomla! Component Sponsor Wall 7.0 - 'wallid' SQL Injection
| php/webapps/413[01;31m[K25[m[K.txt

Joomla! Component Sponsor Wall 8.0 - SQL Injection
| php/webapps/4[01;31m[K25[m[K[01;31m[K25[m[K.txt

Joomla! Component vWishlist 1.0.1 - SQL Injection
| php/webapps/462[01;31m[K25[m[K.txt

Joomla! Component Zap Calendar Lite 4.3.4 - SQL Injection
| php/webapps/4[01;31m[K25[m[K00.txt

Joovili 2.1 - 'members_help.php' Remote File Inclusion
| php/webapps/311[01;31m[K25[m[K.txt

JoWood Chaser 1.0/1.50 - Remote Buffer Overflow
| multiple/remote/[01;31m[K25[m[K191.txt

jPORTAL 2.3.1 - 'Banner.php' SQL Injection
| php/webapps/[01;31m[K25[m[K382.txt

JShop 1.x < 2.x - 'xPage' Local File Inclusion
| php/webapps/53[01;31m[K25[m[K.txt

Jungo DriverWizard WinDriver < 12.4.0 - Kernel Out-of-Bounds Write
Privilege Escalation                    |
windows/local/426[01;31m[K25[m[K.py

Juniper Junos 8.5/9.0 J - Web Interface 'PATH_INFO' Cross-Site
Scripting                                   |
hardware/remote/33[01;31m[K25[m[K7.txt

Juniper Junos 8.5/9.0 J-Web Interface - '/configuration' Multiple
Cross-Site Scripting Vulnerabilities     |
hardware/remote/33[01;31m[K25[m[K9.txt
```

Juniper Junos 8.5/9.0 J-Web Interface - '/diagnose' Multiple Cross-Site Scripting Vulnerabilities | hardware/remote/33[01;31m[K25[m[K8.txt

Just William's Amazon Webstore - 'Closeup.php?Image' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K560.txt

Just William's Amazon Webstore - 'CurrentIsExpanded' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K564.txt

Just William's Amazon Webstore - 'CurrentNumber' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K566.txt

Just William's Amazon Webstore - 'searchFor' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K565.txt

Just William's Amazon Webstore - HTTP Response Splitting | php/webapps/[01;31m[K25[m[K567.txt

JV2 Folder Gallery 3.0 - 'download.php' Remote File Disclosure | php/webapps/31[01;31m[K25[m[K.c

K-COLLECT CSV_DB.CGI 1.0/i_DB.CGI 1.0 - Remote Command Execution | php/webapps/[01;31m[K25[m[K904.c

Kaspersky Internet Security - Remote Denial of Service | windows/dos/391[01;31m[K25[m[K.html

Katello (RedHat Satellite) - users/update_roles Missing Authorisation (Metasploit) | linux/remote/3[01;31m[K25[m[K15.rb

Kayako ESupport 2.3 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/[01;31m[K25[m[K[01;31m[K25[m[K7.txt

Kayako eSupport 2.x - 'index.php' Knowledgebase Cross-Site Scripting | php/webapps/[01;31m[K25[m[K037.txt

Kayako eSupport 2.x - Ticket System Multiple SQL Injections | php/webapps/[01;31m[K25[m[K038.txt

KC Wiki 1.0 - '/simplest/wiki.php?page' Remote File Inclusion | php/webapps/313[01;31m[K25[m[K.txt

KCFinder 2.2 - Arbitrary File Upload | php/webapps/15[01;31m[K25[m[K4.txt

KDE KMail 1.7.1 - HTML EMail Remote Email Content Spoofing | linux/remote/[01;31m[K25[m[K375.pl

KDE Konqueror 3.0.3 - Malformed HTML Page Denial of Service
| linux/dos/2[01;31m[K25[m[K60.txt

KDPics 1.11/1.16 - 'galeries.inc.php3?categories' Cross-Site Scripting
| php/webapps/29[01;31m[K25[m[K5.txt

KDPics 1.11/1.16 - 'index.php3?categories' Cross-Site Scripting
| php/webapps/29[01;31m[K25[m[K4.txt

Kemana Directory 1.5.6 - 'qvc_init()' Cookie Poisoning CAPTCHA Bypass
| php/webapps/3[01;31m[K25[m[K10.txt

Kemana Directory 1.5.6 - 'task.php' Local File Inclusion
| php/webapps/3[01;31m[K25[m[K08.txt

Kemana Directory 1.5.6 - Database Backup Disclosure
| php/webapps/3[01;31m[K25[m[K09.txt

Kemana Directory 1.5.6 - kemana_admin_passwd Cookie User Password Hash
Disclosure |
php/webapps/3[01;31m[K25[m[K06.txt

Kemana Directory 1.5.6 - Remote Code Execution
| php/webapps/3[01;31m[K25[m[K07.txt

Kerio Personal Firewall 4.0.x - Web Filtering Remote Denial of Service
| windows/dos/239[01;31m[K25[m[K.txt

Keyvan1 ImageGallery - Database Disclosure
| asp/webapps/[01;31m[K25[m[K661.txt

Kimai 0.9.2.1306-3 - SQL Injection
| php/webapps/[01;31m[K25[m[K606.py

Kimson CMS - 'id' Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K89.html

KingSoft - 'UpdateOcx2.dll SetUninstallName()' Heap Overflow (PoC)
| windows/dos/52[01;31m[K25[m[K.html

Kirby CMS 2.1.0 - Authentication Bypass
| php/webapps/38[01;31m[K25[m[K5.txt

KiteService 1.2020.618.0 - Unquoted Service Path
| windows/local/486[01;31m[K25[m[K.txt

KKE Info Media Kmita Catalogue 2 - 'search.php' Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K43.txt

KKE Info Media Kmita Gallery - Multiple Cross-Site Scripting
Vulnerabilities |
php/webapps/3[01;31m[K25[m[K44.txt

```
Kloxo 6.1.6 - Local Privilege Escalation
| linux/local/[01;31m[K25[m[K406.sh

Kmail 1.9.1 - IMG SRC Remote Denial of Service
| multiple/dos/[01;31m[K25[m[K15.txt

Knowledgeroot (fckeditor) - Arbitrary File Upload
| php/webapps/1[01;31m[K25[m[K06.php

Konica Minolta FTP Utility 1.0 - Remote Command Execution
| windows/remote/38[01;31m[K25[m[K2.py

Konica Minolta FTP Utility 1.00 - (Authenticated) CWD Command Overflow
(SEH) (Metasploit)                  |
windows/remote/38[01;31m[K25[m[K4.rb

konversation irc client 0.15 - Multiple Vulnerabilities
| linux/remote/[01;31m[K25[m[K054.txt

Kubio AI Page Builder 2.5.1 - Local File Inclusion (LFI)
| multiple/webapps/521[01;31m[K25[m[K.py

Kyocera Printer d-COPIA[01;31m[K25[m[K3MF - Directory Traversal (PoC)
| hardware/webapps/48561.txt

LaGarde StoreFront 5.0 Shopping Cart - 'login.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K847.txt

LAME 3.99.5 - 'III_dequantize_sample' Stack Buffer Overflow
| linux/dos/42[01;31m[K25[m[K9.txt

LAME 3.99.5 - 'II_step_one' Buffer Overflow
| linux/dos/42[01;31m[K25[m[K8.txt

Lan Messenger - sending PM 'UNICODE' Overwrite Buffer Overflow (SEH)
| windows/dos/[01;31m[K25[m[K363.py

LANChat Pro Revival 1.666c - UDP Processing Remote Denial of Service
| multiple/dos/[01;31m[K25[m[K081.txt

Land Down Under 800/801 - 'auth.php?m' SQL Injection
| php/webapps/26[01;31m[K25[m[K3.txt

Land Down Under 800/801 - 'plug.php?e' SQL Injection
| php/webapps/26[01;31m[K25[m[K4.txt

Lanius CMS 1.2.14 - Multiple SQL Injections
| php/webapps/4[01;31m[K25[m[K8.txt

LANSA aXes Web Terminal TN5[01;31m[K25[m[K0 - 'axes_default.css' Cross-
Site Scripting                              |
java/webapps/35683.txt
```

Lazybone Studios WiFi Music 1.0 iOS - Multiple Vulnerabilities
| ios/webapps/3[01;31m[K25[m[K58.txt

LBL Traceroute 1.4 a5 - Heap Corruption (1)
| linux/local/20[01;31m[K25[m[K0.c

LBL Traceroute 1.4 a5 - Heap Corruption (2)
| linux/local/20[01;31m[K25[m[K1.c

LBL Traceroute 1.4 a5 - Heap Corruption (3)
| linux/local/20[01;31m[K25[m[K2.c

Leica Geosystems GR10/GR[01;31m[K25[m[K/GR30/GR50 GNSS 4.30.063 -
Cross-Site Request Forgery |
windows/webapps/46090.html

Leica Geosystems GR10/GR[01;31m[K25[m[K/GR30/GR50 GNSS 4.30.063 -
JS/HTML Code Injection |
windows/webapps/46091.html

Leksbot 1.2 - Multiple Vulnerabilities
| linux/local/2[01;31m[K25[m[K67.c

LeptonCMS 4.5.0 - Persistent Cross-Site Scripting
| php/webapps/48[01;31m[K25[m[K0.txt

LG U8120 Mobile Phone - '.MIDI' File Remote Denial of Service
| hardware/dos/[01;31m[K25[m[K402.txt

Lgames LTris 1.0.1 - Local Memory Corruption
| freebsd/local/2[01;31m[K25[m[K74.pl

Lianja SQL 1.0.0RC5.1 - db_netserver Stack Buffer Overflow (Metasploit)
| windows/remote/[01;31m[K25[m[K851.rb

libbabl 0.1.62 - Broken Double Free Detection (PoC)
| linux/local/49[01;31m[K25[m[K9.c

Liberum Help Desk 0.97.3 - Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K785.txt

libgig 4.0.0 (LinuxSampler) - Multiple Vulnerabilities
| linux/dos/4[01;31m[K25[m[K46.txt

Libopt.a 3.1x - Error Logging Buffer Overflow (1)
| linux/dos/2[01;31m[K25[m[K37.c

Libopt.a 3.1x - Error Logging Buffer Overflow (2)
| linux/local/2[01;31m[K25[m[K38.pl

Library System in PHP 1.0 - 'publisher name' Stored Cross-Site
Scripting (XSS) |
php/webapps/506[01;31m[K25[m[K.txt

```
Libsafe 2.0 - Multi-threaded Process Race Condition Security Bypass
| linux/dos/[01;31m[K25[m[K429.c

libsndfile 1.0.[01;31m[K25[m[K - Local Heap Overflow
| multiple/local/38447.pl

libxml2 2.6.x - 'XMLWriter::writeAttribute()' Memory Leak Information
Disclosure                          |
multiple/remote/35[01;31m[K25[m[K2.php

Liferay CE Portal < 7.1.2 ga3 - Remote Command Execution (Metasploit)
| multiple/webapps/465[01;31m[K25[m[K.rb

Lighthouse Development Squirrelcart 1.5.5 - SQL Injection
| php/webapps/[01;31m[K25[m[K320.txt

LightNEasy 1.2 - no database Remote Hash Retrieve
| php/webapps/54[01;31m[K25[m[K.pl

LinEx - Password Reset
| php/webapps/3[01;31m[K25[m[K61.txt

Link Bid Script - 'links.php' SQL Injection
| php/webapps/1[01;31m[K25[m[K96.txt

Linksys E1500/E[01;31m[K25[m[K00 - 'apply.cgi' Remote Command Injection
(Metasploit)                                        |
hardware/remote/24936.rb

Linksys E1500/E[01;31m[K25[m[K00 - Multiple Vulnerabilities
| hardware/webapps/24475.txt

Linksys PSUS4 PrintServer - POST Denial of Service
| hardware/dos/[01;31m[K25[m[K082.txt

Linksys Routers - LanD Packet Denial of Service
| hardware/dos/268[01;31m[K25[m[K.txt

Linksys WAG54GS 1.0.6 (Wireless-G ADSL Gateway) - 'setup.cgi' Cross-
Site Scripting                          |
hardware/remote/30[01;31m[K25[m[K4.txt

Linksys WET11 - Password Update Remote Authentication Bypass
| hardware/remote/[01;31m[K25[m[K359.txt

Linksys WRT160N - 'apply.cgi' Cross-Site Scripting
| hardware/remote/3[01;31m[K25[m[K99.txt

Linksys WRT160N v2 - 'apply.cgi' Remote Command Injection (Metasploit)
| hardware/remote/[01;31m[K25[m[K608.rb
```

```
Linksys WVBR0-[01;31m[K25[m[K - User-Agent Command Execution
(Metasploit)                                                |
hardware/remote/43429.rb

LinPHA 1.3.4 - Multiple Vulnerabilities
| php/webapps/31[01;31m[K25[m[K6.txt

LinPopUp 1.2 - Remote Buffer Overflow
| linux/remote/[01;31m[K25[m[K008.txt

Linux < 4.14.103 / < 4.19.[01;31m[K25[m[K - Out-of-Bounds Read and
Write in SNMP NAT Module                                    |
linux/dos/46477.txt

Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 /
Fedora 22/[01;31m[K25[m[K / CentOS 7.3.1611) - 'ldso_ | linux_x86-
64/local/42275.c

Linux Kernel (Debian 7/8/9/10 / Fedora 23/24/[01;31m[K25[m[K / CentOS
5.3/5.11/6.0/6.8/7.2.1511) - 'ldso_hwcap Stack Cl |
linux_x86/local/42274.c

Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora
23/24/[01;31m[K25[m[K) - 'ldso_dynamic Stack Clash' L |
linux_x86/local/42276.c

Linux Kernel 2.0/2.1/2.2 - 'autofs' Denial of Service
| linux/dos/19[01;31m[K25[m[K0.txt

Linux Kernel 2.2.[01;31m[K25[m[K/2.4.24/2.6.2 - 'mremap()' Local
Privilege Escalation                                        |
linux/local/160.c

Linux Kernel 2.2.[01;31m[K25[m[K/2.4.24/2.6.2 - 'mremap()' Validator
| linux/local/154.c

Linux Kernel 2.2.x/2.3.x/2.4.x/2.5.x/2.6.x - ELF Core Dump Local Buffer
Overflow (PoC)                      | linux/dos/[01;31m[K25[m[K647.sh

Linux Kernel 2.4.30/2.6.11.5 - BlueTooth 'bluez_sock_create' Local
Privilege Escalation                        |
linux/local/[01;31m[K25[m[K289.c

Linux Kernel 2.4.x/2.6.x - BlueTooth Signed Buffer Index (PoC)
| linux/dos/[01;31m[K25[m[K287.c

Linux Kernel 2.4.x/2.6.x - BlueTooth Signed Buffer Index Privilege
Escalation (1)                              |
linux/local/[01;31m[K25[m[K288.c

Linux Kernel 2.4.x/2.6.x - Multiple ISO9660 Filesystem Handling
Vulnerabilities                                 |
linux/dos/[01;31m[K25[m[K234.sh
```

```
Linux Kernel 2.6.10 - File Lock Local Denial of Service
| linux/dos/[01;31m[K25[m[K322.c

Linux Kernel 2.6.32 < 3.x (CentOS 5/6) - 'PERF_EVENTS' Local Privilege
Escalation (1)                      | linux/local/[01;31m[K25[m[K444.c

Linux Kernel 2.6.35 - Network Namespace Remote Denial of Service
| linux/dos/364[01;31m[K25[m[K.txt

Linux Kernel 2.6.9 < 2.6.[01;31m[K25[m[K (RHEL 4) - utrace and ptrace
Local Denial of Service (1)                       | linux/dos/31965.c

Linux Kernel 2.6.9 < 2.6.[01;31m[K25[m[K (RHEL 4) - utrace and ptrace
Local Denial of Service (2)                       | linux/dos/31966.c

Linux Kernel 2.6.x - 'SYS_EPoll_Wait' Local Integer Overflow / Local
Privilege Escalation (1)              |
linux/local/[01;31m[K25[m[K202.c

Linux Kernel 2.6.x - Cryptoloop Information Disclosure
| linux/local/[01;31m[K25[m[K707.txt

Linux Kernel 2.6.x - Proc dentry_unused Corruption Local Denial of
Service                                  |
linux/dos/279[01;31m[K25[m[K.txt

Linux Kernel < 3.8.x - open-time Capability 'file_ns_capable()' Local
Privilege Escalation                 | linux/local/[01;31m[K25[m[K450.c

Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak
| linux/local/443[01;31m[K25[m[K.c

Linux-ATM LES 2.4 - Command Line Argument Buffer Overflow
| linux/local/2[01;31m[K25[m[K40.c

ListProc 8.2.9 - Catmail ULISTPROC_UMASK Buffer Overflow
| freebsd/local/2[01;31m[K25[m[K73.pl

LiteWEB Web Server 2.5 - Authentication Bypass
| php/webapps/[01;31m[K25[m[K787.txt

Live for Speed S1/S2/Demo - '.mpr replay' Local Buffer Overflow
| windows/local/4[01;31m[K25[m[K2.c

Lively Cart - SQL Injection
| multiple/webapps/373[01;31m[K25[m[K.txt

Livingcolor Livingmailing 1.3 - 'login.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K783.txt

LoCal Calendar 1.1 - 'lcUser.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K95.txt
```

Logic Print 2013 - vTable Overwrite Stack Overflow
| windows/remote/[01;31m[K25[m[K835.html

Logics Software LOG-FT - Arbitrary File Disclosure
| windows/remote/[01;31m[K25[m[K336.txt

Login-Reg Members Management PHP 1.0 - Arbitrary File Upload
| php/webapps/4[01;31m[K25[m[K75.txt

LogMeIn 4.0.784 - 'cfgadvanced.html' HTTP Header Injection
| windows/remote/330[01;31m[K25[m[K.txt

LogonBox Limited / Hypersocket Nervepoint Access Manager -
(Unauthenticated) Insecure Direct Object Refere |
multiple/webapps/46[01;31m[K25[m[K4.txt

Logwatch 2.6 Secure Script - Denial of Service
| linux/dos/[01;31m[K25[m[K465.txt

Loki Download Manager 2.0 - 'Catinfo.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K805.txt

Loki Download Manager 2.0 - 'default.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K804.txt

Lynx 2.8 - '.mailcap'/'.mime.type' Local Code Execution
| linux/remote/3[01;31m[K25[m[K30.txt

Lynx 2.8.6dev.13 - Remote Buffer Overflow (PoC)
| multiple/dos/1[01;31m[K25[m[K6.pl

Macally WIFISD2-2A82 2.000.010 - Guest to Root Privilege Escalation
| hardware/webapps/49[01;31m[K25[m[K6.py

Macromedia ColdFusion MX 6.0 - Error Message Full Path Disclosure
| cfm/webapps/2[01;31m[K25[m[K44.txt

Macromedia ColdFusion MX 6.0 - SQL Error Message Cross-Site Scripting
| cfm/webapps/23[01;31m[K25[m[K6.txt

Macs Framework 1.14f CMS - Persistent Cross-Site Scripting
| php/webapps/483[01;31m[K25[m[K.txt

Magic Calendar Lite 1.02 - 'index.php' SQL Injection
| php/webapps/27[01;31m[K25[m[K1.txt

Magic Music Editor - '.cda' Denial of Service
| windows/dos/16[01;31m[K25[m[K5.pl

Magic Photo Storage Website -
'/user/delete_category.php?_config[site_path]' Remote File Inclusion
| php/webapps/294[01;31m[K25[m[K.txt

```
Magic Winmail Server 4.0 (Build 1112) - 'download.php' Traversal
Arbitrary File Access                       |
php/webapps/[01;31m[K25[m[K064.txt

Magic Winmail Server 4.0 (Build 1112) - 'upload.php' Traversal
Arbitrary File Upload                       |
php/webapps/[01;31m[K25[m[K065.txt

MagicScripts E-Store Kit-2 PayPal Edition - Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K285.txt

MagicScripts E-Store Kit-2 PayPal Edition - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K286.txt

Magneto Net Resource ActiveX 4.0.0.5 - 'NetShareEnum' Universal
| windows/remote/12[01;31m[K25[m[K0.html

Mail-it Now! Upload2Server 1.5 - Arbitrary File Upload
| php/webapps/26[01;31m[K25[m[K5.php

maluinfo 206.2.38 - 'bb_usage_stats.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K37.pl

Mambo Component bigAPE-Backup 1.1 - Remote File Inclusion
| php/webapps/22[01;31m[K25[m[K.txt

Mambo Component perForms 1.0 - Remote File Inclusion
| php/webapps/20[01;31m[K25[m[K.txt

Mambo Component Remository 3.[01;31m[K25[m[K - Remote File Inclusion
| php/webapps/2172.txt

Mambo Open Source 4.5 - 'index.php?mos_change_template' Cross-Site
Scripting                                   |
php/webapps/238[01;31m[K25[m[K.txt

Mambo Open Source 4.6.2 -
'/administrator/popups/index3pop.php?mosConfig_sitename' Cross-Site
Scripting    | php/webapps/32[01;31m[K25[m[K2.txt

Mambo Open Source 4.6.2 - '/mambots/editors/mostlyce/'
PHP/connector.php?Query String Cross-Site Scripting |
php/webapps/32[01;31m[K25[m[K3.txt

ManageEngine ADManager Plus 6.5.7 - Cross-Site Scripting
| windows_x86-64/webapps/45[01;31m[K25[m[K6.txt

ManageEngine ADManager Plus 6.5.7 - HTML Injection
| windows/webapps/45[01;31m[K25[m[K4.txt

ManageEngine Applications Manager 11.0 < 14.0 - SQL Injection / Remote
Code Execution (Metasploit)         |
windows/remote/467[01;31m[K25[m[K.rb
```

ManageEngine opManager 12.3.150 - Authenticated Code Execution
| windows/webapps/47[01;31m[K25[m[K5.py

Marinet CMS - SQL Injection
| php/webapps/1[01;31m[K25[m[K75.txt

Marinet CMS - SQL Injection / Cross-Site Scripting / HTML Injection
| php/webapps/1[01;31m[K25[m[K77.txt

MASM32 11R - Crash (PoC)
| windows/dos/38[01;31m[K25[m[K9.py

Matrimonial Script - SQL Injection
| php/webapps/4[01;31m[K25[m[K45.txt

Matrimonial Script 2.7 - Authentication Bypass
| php/webapps/4[01;31m[K25[m[K66.txt

MAXdev MD-Pro 1.0.73 - Arbitrary File Upload
| php/webapps/262[01;31m[K25[m[K.txt

Maxthon Web Browser 1.2 - Search Bar Information Disclosure
| windows/remote/[01;31m[K25[m[K274.html

Maxthon3 - about:history XCS Trusted Zone Code Execution (Metasploit)
| windows/remote/232[01;31m[K25[m[K.rb

Maxwebportal 1.3 - 'custom_link.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K589.txt

Maxwebportal 1.3 - 'dl_popular.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K585.txt

Maxwebportal 1.3 - 'dl_toprated.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K588.txt

Maxwebportal 1.3 - 'links_popular.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K586.txt

Maxwebportal 1.3 - 'pic_popular.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K587.txt

Maxwebportal 1.3x - 'post.asp' Multiple Cross-Site Scripting
Vulnerabilities |
asp/webapps/[01;31m[K25[m[K651.txt

MayGion IP Cameras Firmware 09.27 - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K25[m[K813.txt

McAfee IntruShield Security Management System - Multiple
Vulnerabilities |
jsp/webapps/[01;31m[K25[m[K946.txt

McGallery 1.0/1.1 - Lang Argument File Disclosure
| php/webapps/[01;31m[K25[m[K823.txt

McNews 1.x - 'install.php' Arbitrary File Inclusion
| php/webapps/[01;31m[K25[m[K232.txt

MDaemon Mailer Daemon 11.0.1 - Remote File Disclosure
| windows/remote/1[01;31m[K25[m[K11.txt

MDaemon WebAdmin 2.0.x - SQL Injection
| windows/webapps/102[01;31m[K25[m[K.txt

MDG Web Server 4D 3.6 - HTTP Command Buffer Overflow
| windows/remote/2[01;31m[K25[m[K56.c

Mega File Manager 1.0 - 'index.php' Local File Inclusion
| php/webapps/90[01;31m[K25[m[K.txt

MegaBook 2.0/2.1 - 'Admin.cgi?EntryID' Cross-Site Scripting
| cgi/webapps/[01;31m[K25[m[K622.txt

Memcached 1.5.5 - 'Memcrashed' Insufficient Control Network Message
Volume Denial of Service (2) |
linux/dos/44[01;31m[K25[m[K4.py

Mensajeitor 1.8.9 - 'IP' HTML Injection
| php/webapps/[01;31m[K25[m[K909.txt

MercuryBoard 1.1 - 'index.php' SQL Injection
| php/webapps/[01;31m[K25[m[K093.txt

MercuryBoard 1.1 - Multiple Input Validation Vulnerabilities
| php/webapps/[01;31m[K25[m[K059.txt

MercuryBoard Forum 1.0/1.1 - Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K112.txt

MercurySteam Scrapland Game Server 1.0 - Remote Denial of Service
| multiple/dos/[01;31m[K25[m[K171.txt

Mesh Viewer 0.2.2 - Remote Buffer Overflow
| windows/remote/[01;31m[K25[m[K026.txt

MetaBid Auctions - 'intAuctionID' SQL Injection
| asp/webapps/[01;31m[K25[m[K544.txt

MetaCart E-Shop - 'ProductsByCategory.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K667.txt

MetaCart E-Shop V-8 - 'IntProdID' SQL Injection
| asp/webapps/[01;31m[K25[m[K536.txt

MetaCart E-Shop V-8 - 'StrCatalog_NAME' SQL Injection
| asp/webapps/[01;31m[K25[m[K537.txt

MetaCart2 - 'CurCatalogID' SQL Injection
| asp/webapps/[01;31m[K25[m[K541.txt

MetaCart2 - 'IntCatalogID' SQL Injection
| asp/webapps/[01;31m[K25[m[K539.txt

MetaCart2 - 'SearchAction.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K543.txt

MetaCart2 - 'StrSubCatalogID' SQL Injection
| asp/webapps/[01;31m[K25[m[K540.txt

MetaCart2 - 'strSubCatalog_NAME' SQL Injection
| asp/webapps/[01;31m[K25[m[K542.txt

Michael Kohn Ringtone Tools 2.22 - '.EMelody' File Remote Buffer
Overflow |
linux/remote/[01;31m[K25[m[K015.txt

Michael Kohn VB2C 0.02 - '.FRM' File Remote Buffer Overflow
| windows/remote/[01;31m[K25[m[K020.txt

Michael Lamont Savant HTTP Server 2.1 - Directory Traversal
| windows/remote/208[01;31m[K25[m[K.txt

Microburst uStorekeeper 1.x - Arbitrary Commands
| cgi/remote/207[01;31m[K25[m[K.txt

Microsoft 'Shlwapi.dll' 6.0.2800.1106 - Malformed HTML Form Tag Denial
of Service |
windows/dos/2[01;31m[K25[m[K18.html

Microsoft .NET Framework EncoderParameter - Integer Overflow (MS12-
0[01;31m[K25[m[K) |
windows/dos/18777.txt

Microsoft Active Directory LDAP Server - 'Username' Enumeration
| windows/remote/3[01;31m[K25[m[K86.py

Microsoft ASP.NET 1.0/1.1 - RPC/Encoded Remote Denial of Service
| asp/dos/[01;31m[K25[m[K962.xml

Microsoft ASP.NET 1.0/1.1 - Unicode Character Conversion Multiple
Cross-Site Scripting Vulnerabilities |
asp/webapps/[01;31m[K25[m[K110.txt

Microsoft BizTalk Server 2000/2002 DTA - 'RawCustomSearchField.asp' SQL
Injection | asp/webapps/2[01;31m[K25[m[K55.txt

```
Microsoft BizTalk Server 2000/2002 DTA - 'rawdocdata.asp' SQL Injection
| asp/webapps/2[01;31m[K25[m[K54.txt

Microsoft BizTalk Server 2002 - HTTP Receiver Buffer Overflow
| windows/dos/2[01;31m[K25[m[K53.txt

Microsoft Data Access Components (MDAC) 2.1 / Microsoft IIS 3.0/4.0 /
Microsoft Index Server 2.0 / Microso |
windows/local/194[01;31m[K25[m[K.txt

Microsoft DebugDiag 1.0 - 'CrashHangExt.dll' ActiveX Control Remote
Denial of Service                    |
windows/dos/3[01;31m[K25[m[K50.html

Microsoft Edge - CMarkup::EnsureDeleteCFState Use-After-Free (MS15-
1[01;31m[K25[m[K)                                |
windows/dos/40878.txt

Microsoft Excel - Malformed FEATHEADER Record (MS09-067) (Metasploit)
| windows/local/166[01;31m[K25[m[K.rb

Microsoft Excel 2007 - WriteAV Crash (PoC)
| windows/dos/2[01;31m[K25[m[K91.txt

Microsoft IIS - Short File/Folder Name Disclosure
| windows/webapps/195[01;31m[K25[m[K.txt

Microsoft IIS 5.0 - User Existence Disclosure (1)
| windows/remote/2[01;31m[K25[m[K62.pl

Microsoft IIS 5.0 - User Existence Disclosure (2)
| windows/remote/2[01;31m[K25[m[K63.pl

Microsoft Internet Explorer (Windows XP SP2) - 'VML' Remote Buffer
Overflow                              |
windows/remote/24[01;31m[K25[m[K.html

Microsoft Internet Explorer - CGenericElement Object Use-After-Free
(Metasploit)                          |
windows/remote/[01;31m[K25[m[K294.rb

Microsoft Internet Explorer - JavaScript 'window()' Crash
| windows/dos/10[01;31m[K25[m[K.html

Microsoft Internet Explorer -
MSHTML!CMultiReadStreamLifetimeManager::ReleaseThreadStateInternal Read
AV   | windows/dos/40[01;31m[K25[m[K3.html

Microsoft Internet Explorer - textNode Use-After-Free (MS13-037)
(Metasploit)                            |
windows/remote/[01;31m[K25[m[K999.rb
```

Microsoft Internet Explorer 11 (Windows 7 x86) - 'mshtml.dll' Remote Code Execution (MS17-007) | windows_x86/remote/431[01;31m[K25[m[K.html

Microsoft Internet Explorer 11.371.16299.0 (Windows 10) - Denial Of Service | windows/dos/445[01;31m[K25[m[K.py

Microsoft Internet Explorer 5 - Remote 'URLMON.dll' Remote Buffer Overflow | windows/remote/2[01;31m[K25[m[K30.pl

Microsoft Internet Explorer 5.0.1 - '.JPEG' Image Rendering Buffer Overflow | windows/dos/[01;31m[K25[m[K991.txt

Microsoft Internet Explorer 5.0.1 - '.JPEG' Image Rendering CMP Fencepost Denial of Service | windows/dos/[01;31m[K25[m[K992.txt

Microsoft Internet Explorer 5.0.1 - Content Advisor File Handling Buffer Overflow (MS05-020) | windows/remote/[01;31m[K25[m[K385.cpp

Microsoft Internet Explorer 5.0.1 - DHTML Object Race Condition Memory Corruption | windows/remote/[01;31m[K25[m[K386.txt

Microsoft Internet Explorer 5.0.1 - Mouse Event URI Status Bar Obfuscation | windows/remote/[01;31m[K25[m[K095.txt

Microsoft Internet Explorer 5/6 - 'file://' Request Zone Bypass | windows/remote/2[01;31m[K25[m[K75.txt

Microsoft Internet Explorer 6 - ' ' Address Bar URI Spoofing | php/webapps/3[01;31m[K25[m[K39.html

Microsoft Internet Explorer 6 - DirectX Media Remote Overflow Denial of Service | windows/dos/4[01;31m[K25[m[K1.html

Microsoft Internet Explorer 6 - Internet.HHCtrl Click Denial of Service | windows/dos/28[01;31m[K25[m[K6.html

Microsoft Internet Explorer 6 - Multiple Object ListWidth Property Denial of Service Vulnerabilities | windows/dos/28[01;31m[K25[m[K8.txt

Microsoft Internet Explorer 6 - NMSA.ASFSourceMediaDescription Stack Overflow | windows/dos/28[01;31m[K25[m[K9.txt

Microsoft Internet Explorer 6 - Pop-up Window Title Bar Spoofing
| windows/remote/[01;31m[K25[m[K129.html

Microsoft Internet Explorer 6 - String To Binary Function Denial of
Service |
windows/dos/28[01;31m[K25[m[K2.txt

Microsoft Internet Explorer 7/8 - findText Unicode Parsing Crash
| windows/dos/9[01;31m[K25[m[K3.html

Microsoft Jet Engine - '.MDB' File Parsing Stack Overflow
| windows/local/46[01;31m[K25[m[K.txt

Microsoft ListBox/ComboBox Control - 'User32.dll' Buffer Overrun
| windows/local/23[01;31m[K25[m[K5.cpp

Microsoft Log Sink Class - ActiveX Control Arbitrary File Creation
| windows/remote/[01;31m[K25[m[K157.txt

Microsoft MSN Messenger 6.2.0137 - '.png' Remote Buffer Overflow
| windows/remote/[01;31m[K25[m[K094.c

Microsoft Office - OLE Multiple DLL Side Loading Vulnerabilities (MS15-
132/MS16-014/MS16-0[01;31m[K25[m[K/MS16-041/MS16 |
windows/local/41706.rb

Microsoft Office 2003 - '.PPT' Local Buffer Overflow (PoC)
| windows/dos/[01;31m[K25[m[K23.pl

Microsoft Office XP 2000/2002 - HTML Link Processing Remote Buffer
Overflow |
windows/dos/[01;31m[K25[m[K085.txt

Microsoft Outlook 2003 - Web Access Login Form Remote URI redirection
| asp/webapps/[01;31m[K25[m[K084.txt

Microsoft Outlook Express 4.x/5.x/6.0 - Attachment Processing File
Extension Obfuscation |
windows/remote/[01;31m[K25[m[K784.txt

Microsoft Outlook Web Access (OWA) 8.2.[01;31m[K25[m[K4.0 - Information
Disclosure |
windows/webapps/12728.txt

Microsoft Paint - Integer Overflow (Denial of Service) (MS10-005)
| windows/dos/1[01;31m[K25[m[K18.pl

Microsoft PowerPoint 2003 - 'powerpnt.exe' Remote Overflow
| windows/remote/282[01;31m[K25[m[K.c

Microsoft RRAS Service - RASMAN Registry Overflow (MS06-
0[01;31m[K25[m[K) (Metasploit) |
windows/remote/16375.rb

Microsoft RRAS Service - Remote Overflow (MS06-0[01;31m[K25[m[K) (Metasploit) | windows/remote/16364.rb

Microsoft SQL Server 7.0/2000 JET Database Engine 4.0 - Buffer Overrun | windows/dos/2[01;31m[K25[m[K76.txt

Microsoft Visual 6 - 'VDT70.dll NotSafe' Remote Stack Overflow | windows/remote/4[01;31m[K25[m[K9.txt

Microsoft Windows - 'win32k!NtGdiGetTextMetricsW' Kernel Stack Memory Disclosure | windows/dos/422[01;31m[K25[m[K.cpp

Microsoft Windows - Escalate UAC Protection Bypass (Via COM Handler Hijack) (Metasploit) | windows/local/4[01;31m[K25[m[K40.rb

Microsoft Windows - GDI+ DecodeCompressedRLEBitmap Invalid Pointer Arithmetic Out-of-Bounds Write (MS16-09 | windows/dos/40[01;31m[K25[m[K5.txt

Microsoft Windows - GDI+ EMR_EXTTEXTOUTA / EMR_POLYTEXTOUTA Heap Buffer Overflow (MS16-097) | windows/dos/40[01;31m[K25[m[K7.txt

Microsoft Windows - GDI+ ValidateBitmapInfo Invalid Pointer Arithmetic Out-of-Bounds Reads (MS16-097) | windows/dos/40[01;31m[K25[m[K6.txt

Microsoft Windows - RRAS RASMAN Registry Stack Overflow (MS06-0[01;31m[K25[m[K) (Metasploit) | windows/remote/1965.pm

Microsoft Windows - SMB Client-Side Bug (PoC) (MS10-006) | windows/dos/12[01;31m[K25[m[K8.py

Microsoft Windows - SMB2 Negotiate Protocol '0x72' Response Denial of Service | windows/dos/1[01;31m[K25[m[K24.py

Microsoft Windows - SmbRelay3 NTLM Replay (MS08-068) | windows/remote/71[01;31m[K25[m[K.txt

Microsoft Windows - Win32k!EPATHOBJ::pprFlattenRec Uninitialized Next Pointer Testcase | windows/dos/[01;31m[K25[m[K611.txt

Microsoft Windows 10 AppXSvc Deployment Service - Arbitrary File Deletion | windows/local/47[01;31m[K25[m[K3.cpp

Microsoft Windows 7 (x64) - 'afd.sys' Dangling Pointer Privilege Escalation (MS14-040) | windows_x86-64/local/395[01;31m[K25[m[K.py

Microsoft Windows 98/2000 Explorer - Preview Pane Script Injection | windows/remote/[01;31m[K25[m[K454.txt

Microsoft Windows 98SE - 'User32.dll' Icon Handling Denial of Service | windows/dos/[01;31m[K25[m[K737.txt

Microsoft Windows Diagnostics Hub - DLL Load Privilege Escalation (MS16-1[01;31m[K25[m[K) | windows/local/40562.cpp

Microsoft Windows Kernel - 'ATMFD.dll' NamedEscape 0x[01;31m[K25[m[K0C Pool Corruption (MS16-074) | windows/dos/39991.txt

Microsoft Windows Kernel - 'win32k!OffsetChildren' Null Pointer Dereference | windows/dos/390[01;31m[K25[m[K.txt

Microsoft Windows Media Digital Rights Management - ActiveX Control Buffer Overflow (PoC) | windows/dos/308[01;31m[K25[m[K.html

Microsoft Windows Media Player 11.0.0 - '.wav' Crash (PoC) | windows/dos/[01;31m[K25[m[K408.pl

Microsoft Windows Media Player 7.1 - Skin File Code Execution | windows/remote/2[01;31m[K25[m[K70.java

Microsoft Windows Media Player 9.0 - ActiveX Control File Enumeration | windows/remote/[01;31m[K25[m[K032.html

Microsoft Windows Media Player 9.0 - ActiveX Control Media File Attribute Corruption | windows/remote/[01;31m[K25[m[K031.html

Microsoft Windows Media Services - ConnectFunnel Stack Buffer Overflow (MS10-0[01;31m[K25[m[K) (Metasploit) | windows/remote/16333.rb

Microsoft Windows NT 4.0 - Invalid LPC Request Denial of Service (MS00-070) | windows/dos/20[01;31m[K25[m[K4.txt

Microsoft Windows NT 4.0/2000 - LPC Zone Memory Depletion Denial of Service | windows/dos/20[01;31m[K25[m[K5.txt

Microsoft Windows NT 4.0/2000 - NTFS File Hiding | linux/local/21[01;31m[K25[m[K8.bat

Microsoft Windows NT 4.0/2000 Predictable LPC Message Identifier - Multiple Vulnerabilities | windows/local/20[01;31m[K25[m[K7.txt

Microsoft Windows NT/2000/2003/2008/XP/Vista/7/8 - 'EPATHOBJ' Local Ring | windows/local/[01;31m[K25[m[K912.c

Microsoft Windows Outlook Express and Windows Mail - Integer Overflow | windows/dos/1[01;31m[K25[m[K64.txt

Microsoft Windows RRAS - Remote Stack Overflow (MS06-0[01;31m[K25[m[K) (Metasploit) | windows/remote/1940.pm

Microsoft Windows Server 2000 - 'RegEdit.exe' Registry Key Value Buffer Overflow | windows/local/2[01;31m[K25[m[K28.c

Microsoft Windows Server 20[01;31m[K25[m[K JScript Engine - Remote Code Execution (RCE) | windows/remote/52315.py

Microsoft Windows Text Services Framework MSCTF - Multiple Vulnerabilities | windows/local/47[01;31m[K25[m[K8.txt

Microsoft Windows Vista - 'iphlpapi.dll' Local Kernel Buffer Overflow | windows/local/3[01;31m[K25[m[K90.c

Microsoft Windows Vista/2003 - 'UnhookWindowsHookEx' Local Denial of Service | windows/dos/3[01;31m[K25[m[K73.txt

Microsoft Windows XP - 'TSShutdn.exe' Remote Denial of Service | windows/dos/[01;31m[K25[m[K268.txt

Microsoft Windows XP - Local Denial of Service | windows/dos/[01;31m[K25[m[K[01;31m[K25[m[K9.py

Microsoft Windows XP - Redirector Privilege Escalation | windows/local/222[01;31m[K25[m[K.txt

Microsoft Windows XP - Self-Executing Folder | windows/remote/241[01;31m[K25[m[K.txt

Microsoft Windows XP SP2 - 'win32k.sys' Local Privilege Escalation (MS08-0[01;31m[K25[m[K) | windows/local/5518.txt

Microsoft Windows XP/2000 - Internet Protocol Validation Remote Code Execution (1) | windows/dos/[01;31m[K25[m[K383.pl

Microsoft Windows XP/2000 - Internet Protocol Validation Remote Code Execution (2) | windows/remote/[01;31m[K25[m[K384.c

Microsoft Windows XP/2000/2003 - 'winhlp32' Phrase Heap Overflow | windows/remote/[01;31m[K25[m[K050.txt

Microsoft Windows XP/2000/2003 - 'winhlp32' Phrase Integer Overflow | windows/remote/[01;31m[K25[m[K049.txt

Microsoft Windows XP/2000/2003 - Graphical Device Interface Library Denial of Service | windows/dos/[01;31m[K25[m[K231.txt

Microsoft Windows XP/95/98/2000/NT 4.0 - 'Riched20.dll' Attribute Buffer Overflow | windows/dos/22[01;31m[K25[m[K5.txt

Microsoft Windows XP/Vista/2000/2003/2008 Kernel - Usermode Callback Privilege Escalation (MS08-0[01;31m[K25[m[K) (1) | windows/dos/31585.c

Microsys CyberPatrol 4.0 4.003/4.0 4.005 - Insecure Registration | multiple/remote/204[01;31m[K25[m[K.pl

MidiCart PHP - 'Item_List.php?MainGroup' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K620.txt

MidiCart PHP - 'Item_List.php?MainGroup' SQL Injection | php/webapps/[01;31m[K25[m[K615.txt

MidiCart PHP - 'Item_List.php?SecondGroup' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K619.txt

MidiCart PHP - 'Item_List.php?SecondGroup' SQL Injection | php/webapps/[01;31m[K25[m[K616.txt

MidiCart PHP - 'Item_Show.php?Code_No' SQL Injection | php/webapps/[01;31m[K25[m[K617.txt

MidiCart PHP - 'Search_List.php?SearchString' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K618.txt

MidiCart PHP - 'Search_List.php?SearchString' SQL Injection | php/webapps/[01;31m[K25[m[K614.txt

Mike Bobbitt Album.PL 0.61 - Remote Command Execution | cgi/webapps/2[01;31m[K25[m[K45.pl

MiniBB 1.5 - 'news.php' Remote File Inclusion | php/webapps/28[01;31m[K25[m[K1.txt

MiniBB keyword_replacer 1.0 - 'pathToFiles' File Inclusion
| php/webapps/[01;31m[K25[m[K28.txt

miniBloggie 1.0 - 'login.php' SQL Injection
| php/webapps/271[01;31m[K25[m[K.txt

Minichat 6.0 - 'ftag.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K19.txt

MiniManager For Mangos/Trinity Server - Denial of Service
| php/dos/1[01;31m[K25[m[K54.txt

MiniUPnPd 1.0 - Remote Stack Buffer Overflow Remote Code Execution
(Metasploit) |
linux/remote/[01;31m[K25[m[K975.rb

MiniWeb HTTP Server 300 - Crash (PoC)
| windows/dos/[01;31m[K25[m[K418.py

MiniWebsvr 0.0.10 - Directory Traversal / Listing
| windows/remote/1[01;31m[K25[m[K80.txt

MitraStar DSL-100HN-T1/GPT-[01;31m[K25[m[K41GNAC - Privilege Escalation
| hardware/remote/43061.txt

Mitrastar GPT-[01;31m[K25[m[K41GNAC-N1 - Privilege escalation
| hardware/remote/50351.txt

MIVA Merchant 5 - Merchant.MVC Cross-Site Scripting
| cgi/webapps/26[01;31m[K25[m[K6.txt

MKPortal 1.1 - Multiple Input Validation Vulnerabilities
| php/webapps/277[01;31m[K25[m[K.txt

Moa Gallery 1.2.0 - 'p_filename' Remote File Disclosure
| php/webapps/95[01;31m[K25[m[K.txt

ModernGigabyte ModernBill 4.3 - 'Aid' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K378.txt

ModernGigabyte ModernBill 4.3 - 'C_CODE' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K377.txt

ModernGigabyte ModernBill 4.3 - 'news.php' File Inclusion
| php/webapps/[01;31m[K25[m[K376.txt

ModSecurity - Remote Null Pointer Dereference
| multiple/dos/[01;31m[K25[m[K852.py

Mod_NTLM 0.x - Authorisation Format String
| multiple/dos/2[01;31m[K25[m[K14.txt

```
Mod_NTLM 0.x - Authorisation Heap Overflow
| multiple/dos/2[01;31m[K25[m[K12.txt

mod_security 2.1.0 - ASCIIZ byte POST Rules Bypass
| multiple/remote/34[01;31m[K25[m[K.txt

MoinMoin - Arbitrary Command Execution
| php/webapps/[01;31m[K25[m[K304.py

MoinMoin 1.5.8/1.9 - Cross-Site Scripting / Information Disclosure
| java/webapps/3[01;31m[K25[m[K74.txt

Monkey HTTPd 1.1.1 - Crash (PoC)
| linux/dos/[01;31m[K25[m[K837.txt

Mono 1.0.5 - Unicode Character Conversion Multiple Cross-Site Scripting
Vulnerabilities                    | asp/webapps/[01;31m[K25[m[K148.txt

Moodle 3.11.5 - SQLi (Authenticated)
| php/webapps/508[01;31m[K25[m[K.py

Mountain Network Systems WebCart 8.4 - Command Execution
| cgi/remote/211[01;31m[K25[m[K.pl

Mozilla (Multiple Products) - iFrame JavaScript Execution
| linux/dos/27[01;31m[K25[m[K7.html

Mozilla - Maintenance Service Log File Overwrite Privilege Escalation
| windows/local/379[01;31m[K25[m[K.txt

Mozilla Firefox 1.0.6/1.0.7 - iFrame Handling Denial of Service
| multiple/dos/263[01;31m[K25[m[K.txt

Mozilla Firefox 1.0.7 (Mozilla 1.7.12) - Denial of Service
| multiple/dos/1[01;31m[K25[m[K7.html

Mozilla Firefox 1.0.7 / Thunderbird 1.0.6 - Denial of Service
| multiple/dos/1[01;31m[K25[m[K3.html

Mozilla Firefox 1.0.x/1.5 - HTML Parsing Denial of Service
| linux/dos/27[01;31m[K25[m[K3.txt

Mozilla Suite And Firefox - DOM Property Overrides Code Execution
| multiple/remote/[01;31m[K25[m[K670.html

Mozilla Suite/Firefox - JavaScript Lambda Replace Heap Memory
Disclosure                                    |
linux/dos/[01;31m[K25[m[K334.txt

Mozilla Suite/Firefox/Thunderbird - Nested Anchor Tag Status Bar
Spoofing                                  |
linux/remote/[01;31m[K25[m[K221.txt
```

MP3 WAV to CD Burner 1.4.24 - Local Buffer Overflow (SEH)
| windows/local/4[01;31m[K25[m[K51.py

MPCSoftWeb 1.0 - Database Disclosure
| asp/webapps/2[01;31m[K25[m[K13.txt

Mtp-Target 1.2.2 Client - Remote Format String
| multiple/remote/[01;31m[K25[m[K574.txt

Mtp-Target Server 1.2.2 - Memory Corruption
| multiple/dos/[01;31m[K25[m[K584.txt

Multiple Browsers - 'history.go()' Denial of Service
| osx/dos/1[01;31m[K25[m[K08.html

Multiple Browsers - 'window.print()' Denial of Service
| osx/dos/1[01;31m[K25[m[K09.html

Multiple Tripwire Interactive Games - 'STEAMCLIENTBLOB' Multiple Denial
of Service Vulnerabilities | windows/dos/34[01;31m[K25[m[K1.txt

Multiple Vendor - TCP Session Acknowledgement Number Denial of Service
| multiple/dos/[01;31m[K25[m[K439.c

Multiple Vendor ICMP Implementation - Malformed Path MTU Denial of
Service |
multiple/dos/[01;31m[K25[m[K388.txt

Multiple Vendor ICMP Implementation - Spoofed Source Quench Packet
Denial of Service |
multiple/dos/[01;31m[K25[m[K387.txt

Multiple Vendor ICMP Message Handling - Denial of Service
| multiple/dos/[01;31m[K25[m[K389.txt

Multiple Vendor Telnet Client - Env_opt_add Heap Buffer Overflow
| linux/dos/[01;31m[K25[m[K303.txt

mUnky 0.01 - 'index.php' Remote Code Execution
| php/webapps/32[01;31m[K25[m[K0.py

MunzurSoft Wep Portal W3 - 'kat' SQL Injection
| asp/webapps/67[01;31m[K25[m[K.txt

MuOnline Loopholes Web Server - 'pkok.asp' SQL Injection
| asp/webapps/1[01;31m[K25[m[K2.html

MuPDF < 200911[01;31m[K25[m[K231942 - 'pdf_shade4.c' Multiple Stack
Buffer Overflows |
windows/local/10244.txt

Mutiny 5 - Arbitrary File Upload (Metasploit)
| linux/remote/[01;31m[K25[m[K517.rb

MVNForum 1.0 - Search Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K438.txt

MWChat 6.7 - 'Start_Lobby.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K786.txt

mxBB Module newssuite 1.03 - Remote File Inclusion
| php/webapps/29[01;31m[K25[m[K.pl

My Kazaam Notes Management System - Multiple Vulnerabilities
| php/webapps/143[01;31m[K25[m[K.txt

My Little Forum 1.5 - 'SearchString' SQL Injection
| php/webapps/12[01;31m[K25[m[K.php

My Video Converter 1.5.24 - Local Buffer Overflow (SEH)
| windows/local/4[01;31m[K25[m[K50.py

MyBB 1.4.2 - 'moderation.php' Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K35.txt

MyBB 1.6 - Full Path Disclosure
| php/webapps/153[01;31m[K25[m[K.txt

MyBB 1.8.[01;31m[K25[m[K - Chained Remote Command Execution
| php/webapps/49696.js

MyBB 1.8.[01;31m[K25[m[K - Poll Vote Count SQL Injection
| php/webapps/49699.txt

MyBB AwayList Plugin - 'index.php?id' SQL Injection
| php/webapps/236[01;31m[K25[m[K.txt

MyBB Extended Useradmininfo Plugin 1.2.1 - Cross-Site Scripting
| php/webapps/315[01;31m[K25[m[K.txt

MyBB User Profile Skype ID Plugin 1.0 - Persistent Cross-Site Scripting
| php/webapps/234[01;31m[K25[m[K.txt

MyBloggie 2.1 - 'index.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K612.txt

MyBulletinBoard (MyBB) RC4 - Multiple Cross-Site Scripting / SQL
Injections |
php/webapps/[01;31m[K25[m[K779.txt

MyGuestbook 0.6.1 - 'Form.Inc.php3' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K941.txt

MyServer 0.8 - Cross-Site Scripting
| windows/remote/[01;31m[K25[m[K646.txt

```
MySpace Uploader - 'MySpaceUploader.ocx 1.0.0.4' Remote Buffer Overflow
| windows/remote/50[01;31m[K25[m[K.html

MySQL 3.20.32/3.22.x/3.23.x - Null Root Password Weak Default
Configuration (1)                                |
linux/remote/217[01;31m[K25[m[K.c

MySQL 3.x/4.0.x - Weak Password Encryption
| linux/local/2[01;31m[K25[m[K65.c

MySQL 4.1/5.0 - Authentication Bypass
| multiple/remote/24[01;31m[K25[m[K0.pl

MySQL 4.x - CREATE FUNCTION Arbitrary libc Code Execution
| multiple/remote/[01;31m[K25[m[K209.pl

MySQL 4.x - CREATE FUNCTION mysql.func Table Arbitrary Library
Injection                                        |
multiple/remote/[01;31m[K25[m[K210.php

MySQL 4.x - CREATE Temporary TABLE Symlink Privilege Escalation
| multiple/remote/[01;31m[K25[m[K211.c

MySQLDumper 1.24.4 - 'restore.php?Filename' Cross-Site Scripting
| php/webapps/371[01;31m[K25[m[K.txt

n@board 3.1.9e - 'naboard_pnr.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K14.txt

Nagios Incident Manager 2.0.0 - Multiple Vulnerabilities
| php/webapps/40[01;31m[K25[m[K2.txt

Nagios Log Server 1.4.1 - Multiple Vulnerabilities
| php/webapps/40[01;31m[K25[m[K0.txt

Nagios Network Analyzer 2.2.0 - Multiple Vulnerabilities
| php/webapps/40[01;31m[K25[m[K1.txt

Nagios XI Version 2024R1.01 - SQL Injection
| multiple/webapps/519[01;31m[K25[m[K.py

NASM 0.98.x - Error Preprocessor Directive Buffer Overflow
| linux/remote/[01;31m[K25[m[K005.txt

NEC Electra Elite IPK II WebPro 01.03.01 - Session Enumeration
| hardware/webapps/484[01;31m[K25[m[K.txt

NeoTracePro 3.[01;31m[K25[m[K - ActiveX 'TraceTarget()' Remote Buffer
Overflow                                             |
windows/remote/4158.html

Neslo Desktop Rover 3.0 - Malformed Packet Remote Denial of Service
| multiple/dos/[01;31m[K25[m[K470.txt
```

Netcomm NB1300 Modem/Router - Remote Denial of Service
| hardware/dos/[01;31m[K25[m[K277.txt

neteyes nexusway border gateway - Multiple Vulnerabilities
| cgi/remote/[01;31m[K25[m[K648.txt

Netgear DGN1000 / DGN2200 - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K25[m[K978.txt

Netgear DGN2200 - 'dnslookup.cgi' Command Injection (Metasploit)
| cgi/remote/42[01;31m[K25[m[K7.rb

Netgear SSL312 PROSAFE SSL VPN-Concentrator [01;31m[K25[m[K - Error
Page Cross-Site Scripting |
hardware/remote/30673.txt

Netgear WGR614 - Administration Interface Remote Denial of Service
| hardware/dos/3[01;31m[K25[m[K83.txt

Netgear WNR500 Wireless Router - 'webproc?getpage' Traversal Arbitrary
File Access |
hardware/webapps/353[01;31m[K25[m[K.txt

Netgear WPN824v3 - Unauthorized Configuration Download
| hardware/webapps/[01;31m[K25[m[K969.txt

NethServer 7.3.1611 - Cross-Site Request Forgery (Create User / Enable
SSH Access) |
json/webapps/4[01;31m[K25[m[K80.html

NethServer 7.3.1611 - Cross-Site Request Forgery / Cross-Site Scripting
| json/webapps/4[01;31m[K25[m[K79.txt

Netis E1+ 1.2.3[01;31m[K25[m[K33 - Backdoor Account (root)
| hardware/webapps/48382.txt

Netis E1+ V1.2.3[01;31m[K25[m[K33 - Unauthenticated WiFi Password Leak
| hardware/webapps/48384.txt

netjukebox 4.01B/5.[01;31m[K25[m[K - 'skin' Cross-Site Scripting
| php/webapps/35499.txt

Netlink GPON Router 1.0.11 - Remote Code Execution
| hardware/webapps/482[01;31m[K25[m[K.txt

NetOffice Dwins 1.4p3 - SQL Injection
| php/webapps/2[01;31m[K25[m[K90.txt

Netquery 3.1 - 'submit.php?portnum' Cross-Site Scripting
| php/webapps/260[01;31m[K25[m[K.txt

Netref 4.2 - 'Cat_for_gen.php' Remote PHP Script Injection
| php/webapps/[01;31m[K25[m[K467.txt

```
Netrw 1[01;31m[K25[m[K Vim Script - Multiple Command Execution
Vulnerabilities                                          |
linux/remote/32012.txt

Netscape Directory Server 4.12 - Directory Server Directory Traversal
| windows/remote/203[01;31m[K25[m[K.txt

Netscape Navigator 7.2 - Infinite Array Sort Denial of Service
| multiple/dos/[01;31m[K25[m[K056.html

Netvidade engine 1.0 - Multiple Vulnerabilities
| php/webapps/1[01;31m[K25[m[K50.pl

NetWin Surgemail 3.8k4-4 - IMAP (Authenticated) Remote LIST Universal
| windows/remote/5[01;31m[K25[m[K9.py

News Evolution 3.0.3 - _NE[AbsPath] Remote File Inclusion
| php/webapps/23[01;31m[K25[m[K.txt

Newsgrab 0.5.0pre4 - Multiple Local/Remote Vulnerabilities
| linux/remote/[01;31m[K25[m[K080.txt

NewsOffice 2.0.18 - 'news_show.php' Cross-Site Scripting
| php/webapps/34[01;31m[K25[m[K8.txt

Newspost 2.0/2.1 - Remote Buffer Overflow
| linux/dos/[01;31m[K25[m[K077.txt

Newsscript - Access Validation
| cgi/webapps/[01;31m[K25[m[K201.txt

NEXTWEB (i)Site - 'login.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K781.txt

Nginx 1.3.9 < 1.4.0 - Chuncked Encoding Stack Buffer Overflow
(Metasploit)                                       |
linux/remote/[01;31m[K25[m[K775.rb

Nginx 1.3.9 < 1.4.0 - Denial of Service (PoC)
| linux/dos/[01;31m[K25[m[K499.py

ngIRCd 0.6/0.7/0.8 - Remote Buffer Overflow
| linux/dos/[01;31m[K25[m[K070.c

Nitro PDF Reader 1.4.0 - Heap Memory Corruption (PoC)
| windows/dos/16[01;31m[K25[m[K4.txt

No-IP Dynamic Update Client (DUC) 2.1.9 - Local IP Address Stack
Overflow                                           |
linux/local/[01;31m[K25[m[K411.py
```

Noah's Classifieds 1.0/1.3 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/27[01;31m[K25[m[K9.txt

Noah's Classifieds 1.2/1.3 - 'index.php' SQL Injection
| php/webapps/26[01;31m[K25[m[K9.txt

Nokia 9500 - vCard Viewer Remote Denial of Service
| hardware/dos/[01;31m[K25[m[K736.txt

Nokia Affix 2.0/2.1/3.x - BTSRV/BTOBEX Remote Command Execution
| hardware/remote/[01;31m[K25[m[K966.txt

Nokia IPSO 3.4.x - Voyager ReadFile.TCL Remote File Reading
| hardware/remote/2[01;31m[K25[m[K33.txt

Nosque Workshop MsgCore 1.9 - Denial of Service
| windows/dos/197[01;31m[K25[m[K.txt

Novell Groupwise Client 8.0 - Multiple Remote Code Execution Vulnerabilities |
multiple/remote/38[01;31m[K25[m[K0.html

Novell NetMail 3.x - Automatic Script Execution
| windows/remote/[01;31m[K25[m[K948.txt

NoviFlow NoviWare < NW400.2.6 - Multiple Vulnerabilities
| hardware/dos/4[01;31m[K25[m[K18.txt

NPDS 4.8 /5.0 - 'modules.php?Lettre' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K745.txt

NPDS 4.8 < 5.0 - 'admin.php?language' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K742.txt

NPDS 4.8 < 5.0 - 'faq.php?categories' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K750.txt

NPDS 4.8 < 5.0 - 'links.php?Query' SQL Injection
| php/webapps/[01;31m[K25[m[K749.txt

NPDS 4.8 < 5.0 - 'powerpack_f.php?language' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K743.txt

NPDS 4.8 < 5.0 - 'reply.php?image_subject' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K747.txt

NPDS 4.8 < 5.0 - 'reviews.php?title' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K746.txt

NPDS 4.8 < 5.0 - 'sdv_infos.php?sitename' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K744.txt

NPDS 4.8 < 5.0 Glossaire Module - 'terme' SQL Injection
| php/webapps/[01;31m[K25[m[K748.txt

NPDS 4.8/5.0 - 'comments.php?thold' SQL Injection
| php/webapps/[01;31m[K25[m[K671.txt

NPDS 4.8/5.0 - 'pollcomments.php?thold' SQL Injection
| php/webapps/[01;31m[K25[m[K672.txt

NRPE 2.15 - Remote Command Execution
| multiple/remote/329[01;31m[K25[m[K.txt

NSKeyedUnarchiver - Info Leak in Decoding SGBigUTF8String
| multiple/dos/47[01;31m[K25[m[K7.txt

NTFS 3.1 - Master File Table Denial of Service
| windows/dos/42[01;31m[K25[m[K3.html

NTSOFT BBS E-Market Professional - Multiple Cross-Site Scripting
Vulnerabilities (2) |
php/webapps/34[01;31m[K25[m[K7.txt

Nuke - SQL Injection
| php/webapps/107[01;31m[K25[m[K.txt

Nuke BookMarks 0.6 - 'Marks.php' Full Path Disclosure
| php/webapps/[01;31m[K25[m[K282.txt

Nuke BookMarks 0.6 - 'Marks.php' SQL Injection
| php/webapps/[01;31m[K25[m[K284.txt

Nuke BookMarks 0.6 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K283.txt

NukeET 3.0/3.1 - Base64 Codigo Variable Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K642.txt

nullam blog 0.1.2 - Local File Inclusion / File Disclosure / SQL
Injection / Cross-Site Scripting |
php/webapps/96[01;31m[K25[m[K.txt

NullSoft Winamp 5.0 - Malformed ID3v2 Tag Buffer Overflow
| windows/remote/[01;31m[K25[m[K989.txt

NullSoft Winamp 5.0.x - Variant 'IN_CDDA.dll' Remote Buffer Overflow
(PoC) |
windows/dos/[01;31m[K25[m[K061.txt

NuralStorm Webmail 0.98b - 'process.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K61.txt

NUVICO DVR NVDV4 / PdvrAtl Module 'PdvrAtl.DLL 1.0.1.[01;31m[K25[m[K' - Remote Buffer Overflow | windows/remote/4903.html

Nvidia Graphics Driver 8774 - Local Buffer Overflow | linux/local/[01;31m[K25[m[K81.c

NXP Semiconductors MIFARE Classic Smartcard - Multiple Vulnerabilities | multiple/local/3[01;31m[K25[m[K01.txt

O3Read 0.0.3 - HTML Parser Buffer Overflow | linux/remote/[01;31m[K25[m[K010.txt

Ocean12 Calendar Manager 1.0 - Admin Form SQL Injection | php/webapps/[01;31m[K25[m[K469.txt

Ocean12 FAQ Manager Pro - Database Disclosure | php/webapps/7[01;31m[K25[m[K8.txt

Ocean12 Membership Manager Pro - Authentication Bypass | php/webapps/7[01;31m[K25[m[K4.txt

Ocean12 Membership Manager Pro - Cross-Site Scripting | php/webapps/[01;31m[K25[m[K354.txt

Ocean12 Technologies Calendar Manager Pro 1.0 1 - '/admin/main.asp?date' SQL Injection | asp/webapps/278[01;31m[K25[m[K.txt

OCS Inventory NG Server 1.3.1 - 'LOGIN' Remote Authentication Bypass | php/webapps/1[01;31m[K25[m[K20.html

OctoberCMS 1.0.4[01;31m[K25[m[K (Build 4[01;31m[K25[m[K) - Cross-Site Scripting | php/webapps/42978.txt

OFTPD 0.3.x - User Command Buffer Overflow | linux/dos/[01;31m[K25[m[K943.txt

Ohesa Emlak Portal 1.0 - 'satilik.asp?Kategori' SQL Injection | asp/webapps/306[01;31m[K25[m[K.txt

Omer Portal 3.2200604[01;31m[K25[m[K - 'arama_islem.asp' Cross-Site Scripting | asp/webapps/35576.txt

Omni-Secure - 'dir' Multiple File Disclosure Vulnerabilities | php/webapps/380[01;31m[K25[m[K.txt

Onecenter Forum 4.0 - IMG Tag Script Injection | php/webapps/2[01;31m[K25[m[K43.txt

OneWorldStore - 'DisplayResults.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K456.txt

OneWorldStore - 'DisplayResults.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K455.txt

OneWorldStore - 'OWAddItem.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K424.txt

OneWorldStore - 'OWContactUs.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K427.txt

OneWorldStore - 'OWListProduct.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K428.txt

OneWorldStore - 'OWListProduct.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K4[01;31m[K25[m[K.txt

OneWorldStore - 'OWProductDetail.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K426.txt

OneWorldStore - IDOrder Information Disclosure
| asp/webapps/[01;31m[K25[m[K530.txt

Online Inventory Manager 3.2 - Persistent Cross-Site Scripting
| php/webapps/477[01;31m[K25[m[K.txt

Online Learning Management System 1.0 - Multiple Stored XSS
| php/webapps/493[01;31m[K25[m[K.txt

Online Shopping Alphaware 1.0 - Authentication Bypass
| php/webapps/487[01;31m[K25[m[K.txt

Online Store Application Template - 'Sign_In.aspx' SQL Injection
| asp/webapps/304[01;31m[K25[m[K.txt

OOApp Guestbook - Multiple HTML Injection Vulnerabilities
| php/webapps/[01;31m[K25[m[K158.txt

Open Conference Systems 1.1.4 - 'fullpath' File Inclusion
| php/webapps/[01;31m[K25[m[K36.txt

Open Proficy HMI-SCADA 5.0.0.[01;31m[K25[m[K920 - 'Password' Denial of
Service (PoC) | ios/dos/47665.py

Open Solution Quick.Cart 0.3 - 'index.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K650.txt

open-medium.CMS 0.[01;31m[K25[m[K - '404.php' Remote File Inclusion
| php/webapps/1824.txt

openauto 1.6.3 - Multiple Vulnerabilities
| php/webapps/158[01;31m[K25[m[K.txt

```
OpenBB 1.0.8 - 'member.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K657.txt

OpenBB 1.0.8 - 'Read.php' SQL Injection
| php/webapps/[01;31m[K25[m[K656.txt

OpenBB 1.0/1.1 - 'board.php' SQL Injection
| php/webapps/2[01;31m[K25[m[K19.txt

OpenBB 1.0/1.1 - 'index.php' SQL Injection
| php/webapps/2[01;31m[K25[m[K17.txt

OpenBB 1.0/1.1 - 'member.php' SQL Injection
| php/webapps/2[01;31m[K25[m[K20.txt

OpenBSD 2.x - 'fstat' Format String
| openbsd/local/20[01;31m[K25[m[K6.c

OpenBSD 2.x < 3.3 - 'exec_ibcs2_coff_prep_zmagic()' kernel stack
overflow                                  |
bsd/local/1[01;31m[K25[m[K.c

OpenBSD 3.x/4.x - ICMPv6 Packet Handling Remote Buffer Overflow
| openbsd/remote/297[01;31m[K25[m[K.py

OpenCart 1.5.6.1 - 'openbay' Multiple SQL Injections
| php/webapps/3[01;31m[K25[m[K20.txt

OpenConnect WebConnect 6.4/6.5 - jretest.html Traversal Arbitrary File
Access                                    |
windows/remote/[01;31m[K25[m[K146.txt

OpenDock FullCore 4.4 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K70.txt

OpenDocMan 1.2.6.5 - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K[01;31m[K25[m[K0.txt

OpenFiler - 'device' Cross-Site Scripting
| php/webapps/351[01;31m[K25[m[K.txt

OpenNMS 1.5.x - 'filter' Cross-Site Scripting
| jsp/webapps/324[01;31m[K25[m[K.txt

OpenSIS 8.0 'modname' - Directory Traversal
| php/webapps/50[01;31m[K25[m[K9.txt

OpenSSH 1.2 - '.scp' File Create/Overwrite
| linux/remote/20[01;31m[K25[m[K3.sh

OpenSSH/PAM 3.6.1p1 - Remote Users Discovery Tool
| linux/remote/[01;31m[K25[m[K.c
```

OpenTopic 2.3.1 - Private Message HTML Injection
| php/webapps/221[01;31m[K25[m[K.txt

Opera 6.0.x/7.0 - Long File Name Remote Heap Corruption
| windows/dos/2[01;31m[K25[m[K50.pl

Opera 7.0/7.10 - JavaScript Console Single Quote Attribute Injection
| windows/remote/2[01;31m[K25[m[K46.txt

Opera 7.10 - Permanent Denial of Service
| multiple/dos/2[01;31m[K25[m[K36.txt

Opera 7.x/Firefox 1.0/Internet Explorer 6.0 - Information Disclosure
| windows/remote/[01;31m[K25[m[K188.txt

Opera 8.02 - Remote Denial of Service (1)
| multiple/dos/1[01;31m[K25[m[K4.html

Opera 8.02 - Remote Denial of Service (2)
| windows/dos/1[01;31m[K25[m[K5.html

Opera Web Browser 7.53 - Location Replace URI Obfuscation
| multiple/remote/243[01;31m[K25[m[K.html

Opera Web Browser 9.62 - History Search Input Validation
| windows/remote/3[01;31m[K25[m[K55.html

Opera Web Browser 9.x - History Search and Links Panel Cross-Site
Scripting |
linux/remote/3[01;31m[K25[m[K48.html

Ophcrack 3.5.0 - Code Execution Local Buffer Overflow
| windows/local/[01;31m[K25[m[K607.py

Oracle 10g Database - 'SUBSCRIPTION_NAME' SQL Injection (1)
| multiple/remote/[01;31m[K25[m[K452.pl

Oracle 10g Database - 'SUBSCRIPTION_NAME' SQL Injection (2)
| multiple/remote/[01;31m[K25[m[K453.pl

Oracle 8 - oratclsh Suid
| linux/local/191[01;31m[K25[m[K.txt

Oracle 8.x/9.x/10.x Database - Multiple SQL Injections
| multiple/remote/[01;31m[K25[m[K396.txt

Oracle 9i/10g - Database Fine Grained Audit Logging Failure
| multiple/remote/[01;31m[K25[m[K613.txt

Oracle Application Server 9.0 - HTTP Service Mod_Access Restriction
Bypass |
multiple/remote/[01;31m[K25[m[K559.txt

Oracle Application Server 9i - Webcache Cache_dump_file Cross-Site Scripting |
multiple/remote/[01;31m[K25[m[K562.txt

Oracle Application Server 9i - Webcache PartialPageErrorPage Cross-Site Scripting |
multiple/remote/[01;31m[K25[m[K563.txt

Oracle Application Server 9i Webcache - Arbitrary File Corruption
| multiple/remote/[01;31m[K25[m[K561.txt

Oracle AutoVue 20.0.1 - 'AutoVueX.ocx' ActiveX Control 'ExportEdaBom()' Insecure Method |
windows/remote/36[01;31m[K25[m[K0.html

Oracle Database 10.1 - MDSYS.MD2.SDO_CODE_SIZE Buffer Overflow
| multiple/remote/[01;31m[K25[m[K397.txt

Oracle Database 8i/9i - Multiple Directory Traversal Vulnerabilities
| windows/remote/[01;31m[K25[m[K195.txt

Oracle Database Server 9.0.x - Oracle Binary Local Buffer Overflow
| linux/local/23[01;31m[K25[m[K8.c

Oracle Forms and Reports 11.1 - Arbitrary Code Execution
| jsp/remote/31[01;31m[K25[m[K3.rb

Oracle PeopleSoft - 'PeopleSoftServiceListeningConnector' XML External Entity via DOCTYPE |
xml/webapps/419[01;31m[K25[m[K.txt

Oracle Rapid Install Web Server - Secondary Login Page Cross-Site Scripting |
multiple/remote/30[01;31m[K25[m[K6.txt

Oracle Reports Server 10g - Multiple Cross-Site Scripting Vulnerabilities |
jsp/webapps/[01;31m[K25[m[K269.txt

Oracle WebCenter Content - 'CheckOutAndOpen.dll' ActiveX Remote Code Execution (Metasploit) |
windows/remote/[01;31m[K25[m[K979.rb

Oracle9i Application Server 9.0.2 - MOD_ORADAV Access Control
| multiple/remote/[01;31m[K25[m[K988.txt

Orbis CMS 1.0.2 - 'editor-body.php' Cross-Site Scripting
| php/webapps/34[01;31m[K25[m[K3.txt

Orbit Downloader 2.8.7 - Arbitrary File Deletion
| windows/remote/8[01;31m[K25[m[K7.txt

```
Orenosv HTTP/FTP Server 0.8.1 - 'CGISSI.exe' Remote Buffer Overflow
(PoC)                                    |
windows/dos/[01;31m[K25[m[K631.txt

Orenosv HTTP/FTP Server 0.8.1 - FTP Commands Remote Buffer Overflow
| windows/dos/[01;31m[K25[m[K629.pl

Orthanc DICOM Server 1.1.0 - Memory Corruption
| windows/dos/409[01;31m[K25[m[K.py

OS4E - 'login.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K751.txt

OSClass 2.3.3 - 'index.php?sCategory' SQL Injection
| php/webapps/366[01;31m[K25[m[K.txt

osCommerce 2.1/2.2 - Multiple HTTP Response Splitting Vulnerabilities
| php/webapps/[01;31m[K25[m[K840.txt

osCommerce 2.2 - 'Contact_us.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K105.txt

osCommerce 2.2 - 'update.php' Information Disclosure
| php/webapps/[01;31m[K25[m[K994.txt

Osprey 1.0 - 'GetRecord.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K72.txt

Osprey 1.0a4.1 - 'ListRecords.php' Multiple Remote File Inclusions
| php/webapps/3[01;31m[K25[m[K21.txt

osTicket 1.12 - Formula Injection
| php/webapps/472[01;31m[K25[m[K.txt

osTicket 1.14.1 - 'Saved Search' Persistent Cross-Site Scripting
| php/webapps/485[01;31m[K25[m[K.txt

osTicket 1.2/1.3 - 'view.php?inc' Arbitrary Local File Inclusion
| php/webapps/[01;31m[K25[m[K926.txt

osTicket 1.2/1.3 - Multiple Input Validation / Remote Code Injection
Vulnerabilities                          |
php/webapps/[01;31m[K25[m[K590.txt

osTicket STS 1.2 - Attachment Remote Command Execution
| php/webapps/242[01;31m[K25[m[K.php

OutStart Participate Enterprise 3 - Multiple Access Validation
Vulnerabilities                                  |
jsp/webapps/[01;31m[K25[m[K198.txt

Ovidentia FX - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K816.txt
```

P-News 1.16 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K77.txt

P2GChinchilla HTTP Server 1.1.1 - Denial of Service
| windows/dos/11[01;31m[K25[m[K4.pl

PABox 2.0 - Post Icon HTML Injection
| php/webapps/[01;31m[K25[m[K220.txt

paBugs 2.0 Beta 3 - 'main.php?cid' SQL Injection
| php/webapps/4[01;31m[K25[m[K3.pl

PAFaq - Administrator 'Username' SQL Injection
| php/webapps/[01;31m[K25[m[K856.txt

PAFaq - Question Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K854.txt

paFaq beta4 - 'answer.php?offset' SQL Injection
| php/webapps/[01;31m[K25[m[K115.txt

paFaq beta4 - 'comment.php' Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K117.txt

paFaq beta4 - 'question.php' Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K114.txt

paFaq beta4 - 'search.php?search_item' SQL Injection
| php/webapps/[01;31m[K25[m[K116.txt

PAFaq beta4 - Database Unauthorized Access
| php/webapps/[01;31m[K25[m[K848.pl

PAFileDB 1.1.3/2.1.1/3.0/3.1 - 'category.php?start' Cross-Site
Scripting |
php/webapps/[01;31m[K25[m[K216.txt

PAFileDB 1.1.3/2.1.1/3.0/3.1 - 'category.php?start' SQL Injection
| php/webapps/[01;31m[K25[m[K214.txt

PAFileDB 1.1.3/2.1.1/3.0/3.1 - 'viewall.php?start' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K215.txt

PAFileDB 1.1.3/2.1.1/3.0/3.1 - 'viewall.php?start' SQL Injection
| php/webapps/[01;31m[K25[m[K213.txt

PAFileDB 1.1.3/2.1.1/3.0/3.1 - Multiple Input Validation
Vulnerabilities |
php/webapps/[01;31m[K25[m[K824.txt

pagetree CMS 0.0.2 Beta 0001 - Remote File Inclusion
| php/webapps/7[01;31m[K25[m[K5.txt

Panda AntiVirus 2008 - Local Privilege Escalation
| windows/local/4[01;31m[K25[m[K7.c

pandaBB - 'displayCategory' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K99.txt

Pandora FMS 5.0/5.1 - Authentication Bypass
| php/webapps/37[01;31m[K25[m[K5.txt

PaNews 2.0 - Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K111.txt

PANews 2.0 - PHP Remote Code Execution
| php/webapps/[01;31m[K25[m[K145.txt

Papaya CMS 4.0.4 - Cross-Site Scripting
| php/webapps/269[01;31m[K25[m[K.txt

Parallels Virtuozzo Containers 3.0.0-[01;31m[K25[m[K.4.swsoft VZPP
Interface Change Pass - Cross-Site Request Forgery |
php/webapps/31604.html

Parallels Virtuozzo Containers 3.0.0-[01;31m[K25[m[K.4/4.0.0-365.6 VZPP
Interface File Manger - Cross-Site Request Forg |
php/webapps/31603.html

Pargoon CMS - Denial of Service
| multiple/dos/1[01;31m[K25[m[K55.txt

PayProCart 11460784[01;31m[K25[m[K - Multiple Remote File Inclusions
| php/webapps/2316.txt

PBLang Bulletin Board System 4.6 - 'search.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K151.txt

PBLang Bulletin Board System 4.x - 'DelPM.php' Arbitrary Personal
Message Deletion |
php/webapps/[01;31m[K25[m[K179.txt

PBLang Bulletin Board System 4.x - 'SendPM.php' Directory Traversal
| php/webapps/[01;31m[K25[m[K176.txt

PC SOFT WinDEV 11 - '.WDP' File Parsing Stack Buffer Overflow
| windows/dos/30[01;31m[K25[m[K5.txt

PCAL 4.x - Calendar File 'getline' Remote Buffer Overflow
| linux/remote/[01;31m[K25[m[K035.txt

PCAL 4.x - Calendar File 'get_holiday' Remote Buffer Overflow
| linux/remote/[01;31m[K25[m[K036.txt

PCDJ Karaoki 0.6.3819 - Denial of Service
| windows/dos/15[01;31m[K25[m[K7.py

```
PCMan FTP Server 2.07 - 'ABOR' Remote Buffer Overflow
| windows/remote/31[01;31m[K25[m[K4.py

PCMan FTP Server 2.07 - 'CWD' Remote Buffer Overflow
| windows/remote/31[01;31m[K25[m[K5.py

PDF-XChange Viewer 2.5 Build 314.0 - Code Execution
| windows/local/4[01;31m[K25[m[K37.txt

People Can Fly Painkiller Gamespy 1.3 - CD-Key Hash Remote Buffer
Overflow                                  |
multiple/remote/[01;31m[K25[m[K079.txt

Perl 5.10 - Multiple Null Pointer Dereference Denial of Service
Vulnerabilities                           |
multiple/dos/357[01;31m[K25[m[K.pl

PEStudio 3.69 - Denial of Service
| windows/dos/[01;31m[K25[m[K972.py

PGN2WEB 0.3 - Remote Buffer Overflow
| windows/remote/[01;31m[K25[m[K023.txt

PH Pexplorer 0.24 - 'explorer_load_lang.php' Local File Inclusion
| php/webapps/[01;31m[K25[m[K98.php

Phaos 0.9.2 - 'basename()' Remote Command Execution
| php/webapps/2[01;31m[K25[m[K3.php

PHD Help Desk 2.12 - SQL Injection
| php/webapps/[01;31m[K25[m[K915.py

Phoenix Contact WebVisit 29857[01;31m[K25[m[K - Authentication Bypass
| windows/webapps/45590.py

Phorum 3.4.x - 'Message Form' HTML Injection
| php/webapps/2[01;31m[K25[m[K79.txt

Phorum 3.x/5.0.x - HTTP Response Splitting
| php/webapps/[01;31m[K25[m[K[01;31m[K25[m[K8.txt

Phorum 5.0.11 - 'Read.php' SQL Injection
| php/webapps/[01;31m[K25[m[K919.txt

Phorum 5.0.14 - Multiple Subject and Attachment HTML Injection
Vulnerabilities                           |
php/webapps/[01;31m[K25[m[K223.txt

Photodex ProShow Producer 5.0.3[01;31m[K25[m[K6 - Buffer Overflow
| windows/dos/19563.txt
```

```
Photodex ProShow Producer 5.0.3[01;31m[K25[m[K6 - load File Handling
Buffer Overflow (Metasploit)                        |
windows/local/20109.rb

Photodex ProShow Producer 5.0.3[01;31m[K25[m[K6 - Local Buffer Overflow
| windows/local/20036.pl

PhotoGal 1.0/1.5 - News_File Remote File Inclusion
| php/webapps/[01;31m[K25[m[K955.txt

PhotoPost Pro 5.1 - 'showgallery.php' Multiple Cross-Site Scripting
Vulnerabilities                          |
php/webapps/[01;31m[K25[m[K308.txt

PhotoPost Pro 5.1 - 'showmembers.php' Multiple Cross-Site Scripting
Vulnerabilities                          |
php/webapps/[01;31m[K25[m[K309.txt

PhotoPost Pro 5.1 - 'showmembers.php?sl' SQL Injection
| php/webapps/[01;31m[K25[m[K311.txt

PhotoPost Pro 5.1 - 'showphoto.php?photo' SQL Injection
| php/webapps/[01;31m[K25[m[K312.txt

PhotoPost Pro 5.1 - 'Slideshow.php?photo' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K310.txt

PHP 4 - 'PHPInfo()' Cross-Site Scripting
| php/webapps/227[01;31m[K25[m[K.txt

PHP 4.4.6/5.2.1 - ext/gd Already Freed Resources Usage
| linux/local/35[01;31m[K25[m[K.php

PHP 4.x - 'socket_recv()' Signed Integer Memory Corruption
| php/dos/224[01;31m[K25[m[K.php

PHP 4.x/5.0 Shared Memory Module - Offset Memory Corruption
| php/local/[01;31m[K25[m[K040.php

PHP 5.3.1 - 'session_save_path() Safe_mode()' Restriction Bypass
Exploiot                                    |
php/dos/336[01;31m[K25[m[K.php

PHP 5.3.x - Denial of Service
| php/dos/12[01;31m[K25[m[K9.php

PHP 5.4/5.5/5.6 - 'Unserialize()' Use-After-Free
| php/dos/381[01;31m[K25[m[K.txt

PHP Address Book - '/addressbook/register/delete_user.php?id' SQL
Injection                                   |
php/webapps/384[01;31m[K25[m[K.txt
```

PHP Advanced Transfer Manager 1.21 - Arbitrary File Inclusion
| php/webapps/[01;31m[K25[m[K686.txt

PHP Advanced Transfer Manager 1.21 - Arbitrary File Upload
| php/remote/[01;31m[K25[m[K627.txt

PHP AMX 0.90 - '/plugins/main.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K91.txt

PHP Appointment Booking Script - Authentication Bypass
| php/webapps/4[01;31m[K25[m[K83.txt

PHP Arena PAFileDB 3.1 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K200.txt

PHP Chat for 123 Flash Chat - Remote File Inclusion
| php/webapps/144[01;31m[K25[m[K.txt

PHP Classifieds Script 5.6.2 - SQL Injection
| php/webapps/4[01;31m[K25[m[K26.txt

PHP Coupon Script 6.0 - 'cid' SQL Injection
| php/webapps/4[01;31m[K25[m[K28.txt

PHP Designer 2007 Personal - Multiple SQL Injections
| php/webapps/370[01;31m[K25[m[K.txt

PHP JOBWEBSITE PRO - 'forgot.php' Cross-Site Scripting
| php/webapps/326[01;31m[K25[m[K.txt

PHP Jokesite 2.0 - 'joke_id' SQL Injection
| php/webapps/4[01;31m[K25[m[K34.txt

PHP Labs - '.proFile' Dir URI Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K468.txt

PHP Labs - '.proFile' File URI Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K473.txt

PHP Laravel 8.70.1 - Cross Site Scripting (XSS) to Cross Site Request
Forgery (CSRF) |
php/webapps/505[01;31m[K25[m[K.txt

PHP Link Manager 1.7 - URL Redirection
| php/webapps/1[01;31m[K25[m[K34.txt

PHP Live! 3.2.2 - 'questid' SQL Injection (1)
| php/webapps/51[01;31m[K25[m[K.txt

PHP Live! 3.2.2 - 'questid' SQL Injection (2)
| php/webapps/9[01;31m[K25[m[K4.txt

PHP Matrimonial Script 3.0 - SQL Injection
| php/webapps/415[01;31m[K25[m[K.txt

PHP Multi Vendor Script 1.02 - 'sid' SQL Injection
| php/webapps/429[01;31m[K25[m[K.txt

PHP News Reader 2.6.4 - 'phpBB.inc.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K17.pl

PHP Poll Creator 1.0.1 - 'Poll_Vote.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K704.txt

PHP RSS Reader 2010 - SQL Injection
| php/webapps/29[01;31m[K25[m[K8.txt

PHP Search Engine 1.0 - SQL Injection
| php/webapps/4[01;31m[K25[m[K73.txt

PHP Video Battle Script 1.0 - SQL Injection
| php/webapps/4[01;31m[K25[m[K85.txt

PHP-Board 1.0 - User Password Disclosure
| php/webapps/22[01;31m[K25[m[K2.txt

PHP-Charts 1.0 - Code Execution
| php/webapps/[01;31m[K25[m[K496.txt

PHP-Fusion 4.0 - 'Viewthread.php' Information Disclosure
| php/webapps/[01;31m[K25[m[K089.txt

PHP-Fusion 4/5 - 'Setuser.php' HTML Injection
| php/webapps/[01;31m[K25[m[K241.html

PHP-Fusion 5.0 - BBCode IMG Tag Script Injection
| php/webapps/[01;31m[K25[m[K197.txt

PHP-Lance 1.52 - 'subcat' SQL Injection
| php/webapps/4[01;31m[K25[m[K33.txt

PHP-Nuke - 'friend.php' Module SQL Injection
| php/webapps/1[01;31m[K25[m[K[01;31m[K25[m[K.txt

PHP-Nuke 0-7 - Double Hex Encoded Input Validation
| php/webapps/[01;31m[K25[m[K635.txt

PHP-Nuke 5.0 - Viewslink SQL Injection
| php/webapps/1[01;31m[K25[m[K14.txt

PHP-Nuke 5.x/6.x Web_Links Module - SQL Injection
| php/webapps/2[01;31m[K25[m[K89.txt

PHP-Nuke 6.0/6.5 Web_Links Module - Full Path Disclosure
| php/webapps/2[01;31m[K25[m[K98.txt

```
PHP-Nuke 6.5 (Multiple Downloads Module) - SQL Injection
| php/webapps/2[01;31m[K25[m[K97.txt

PHP-Nuke 6.5 - 'modules.php?Username' Cross-Site Scripting
| php/webapps/2[01;31m[K25[m[K95.txt

PHP-Nuke 6.x/7.x 'Downloads' Module - 'Lid' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K341.html

PHP-Nuke 6.x/7.x - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K103.txt

PHP-Nuke 6.x/7.x Your_Account Module - 'Username' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K339.txt

PHP-Nuke 6.x/7.x Your_Account Module - Avatarcategory Cross-Site
Scripting                                  |
php/webapps/[01;31m[K25[m[K340.txt

PHP-Nuke 7.0/8.1/8.1.35 - Wormable Remote Code Execution
| php/webapps/1[01;31m[K25[m[K10.php

PHP-Nuke 7.6 - 'banners.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K343.txt

PHP-Nuke 7.6 Surveys Module - HTTP Response Splitting
| php/webapps/[01;31m[K25[m[K430.txt

PHP-Nuke 7.6 Web_Links Module - Multiple Cross-Site Scripting
Vulnerabilities                            |
php/webapps/[01;31m[K25[m[K342.txt

PHP-Nuke 7.6 Web_Links Module - Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K360.txt

PHP-Nuke Nuke League Module - 'tid' Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K38.txt

PHP-Nuke Splatt Forum 4.0 Module - Cross-Site Scripting
| php/webapps/2[01;31m[K25[m[K57.txt

PHP-Nuke Splatt Forum 4.0 Module - HTML Injection
| php/webapps/2[01;31m[K25[m[K58.txt

PHP-Nuke Web_Links Module - 'cid' SQL Injection
| php/webapps/31[01;31m[K25[m[K2.txt

PHP-Post 1.01 - 'template' Remote Code Execution
| php/webapps/[01;31m[K25[m[K93.php

PHP-RESIDENCE 0.7.2 - 'Search' SQL Injection
| php/webapps/49[01;31m[K25[m[K.txt
```

```
PHP-revista 1.1.2 - Remote File Inclusion / SQL Injection /
Authentication Bypass / Cross-Site Scripting   |
php/webapps/84[01;31m[K25[m[K.txt

PHP-Ring Webring System 0.9.1 - Insecure Cookie Handling
| php/webapps/62[01;31m[K25[m[K.txt

PHP-SecureArea < 2.7 - Multiple Vulnerabilities
| php/webapps/4[01;31m[K25[m[K95.txt

PHPAdsNew 2.0.4 - 'AdFrame.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K2[01;31m[K25[m[K.txt

phpArcadeScript 4 - 'cat' SQL Injection
| php/webapps/6[01;31m[K25[m[K5.txt

phpAuction 2.5 - Multiple Vulnerabilities
| php/webapps/[01;31m[K25[m[K954.txt

PHPBasket - 'pro_id' SQL Injection
| php/webapps/6[01;31m[K25[m[K8.txt

phpBB 1.x/2.0.x - Knowledge Base Module 'KB.php' SQL Injection
| php/webapps/[01;31m[K25[m[K451.txt

phpBB 2.0.13 DLMan Pro Module - SQL Injection
| php/webapps/[01;31m[K25[m[K344.txt

phpBB 2.0.13 Linkz Pro Module - SQL Injection
| php/webapps/[01;31m[K25[m[K345.txt

phpBB 2.0.6 - URL BBCode HTML Injection
| php/webapps/231[01;31m[K25[m[K.txt

phpBB 2.0.x - 'BBCode.php' URL Tag
| jsp/webapps/[01;31m[K25[m[K628.txt

phpBB 2.0.x - 'profile.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K523.txt

phpBB 2.0.x - 'viewtopic.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K524.txt

phpBB 2.0.x - Authentication Bypass (1)
| php/webapps/[01;31m[K25[m[K168.c

phpBB 2.0.x - Authentication Bypass (2)
| php/webapps/[01;31m[K25[m[K169.pl

phpBB 2.0.x - Authentication Bypass (3)
| php/webapps/[01;31m[K25[m[K170.cpp
```

```
phpBB ACP User Registration Mod 1.0 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K51.txt

phpBB Ajax Shoutbox 0.0.5 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K32.txt

phpBB Amazonia Mod - 'zufallscodepart.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K44.pl

phpBB ezBoard Converter 0.2 - 'ezconvert_dir' Remote File Inclusion
| php/webapps/3[01;31m[K25[m[K8.txt

phpBB Import Tools Mod 0.1.4 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K31.txt

phpBB Insert User Mod 0.1.2 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K[01;31m[K25[m[K.pl

phpBB Journals System Mod 1.0.2 RC2 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K22.py

phpBB lat2cyr Mod 1.0.1 - 'lat2cyr.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K46.pl

phpBB Mod Ktauber.com StylesDemo - Blind SQL Injection
| php/webapps/44[01;31m[K25[m[K.pl

phpBB News Defilante Horizontale 4.1.1 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K45.pl

phpBB Notes Module - SQL Injection
| php/webapps/[01;31m[K25[m[K558.txt

phpBB Photo Album 2.0.53 Module - 'Album_Cat.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K403.txt

phpBB Photo Album Module 2.0.53 - 'Album_Comment.php' Cross-Site
Scripting                                  |
php/webapps/[01;31m[K25[m[K404.txt

phpBB PlusXL 2.0_272 - 'constants.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K38.pl

phpBB Prillian French Mod 0.8.0 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K50.pl

phpBB Remote - 'mod.php' SQL Injection
| php/webapps/[01;31m[K25[m[K432.txt

phpBB RPG Events 1.0 - 'functions_rpg_events' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K48.pl
```

```
phpBB SearchIndexer Mod - 'archive_topic.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K49.pl

phpBB Security 1.0.1 - 'PHP_security.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K52.pl

phpBB SpamBlocker Mod 1.0.2 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K33.py

phpBB SpamOborona Mod 1.0b - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K47.pl

phpBB++ Build 100 - 'phpbb_root_path' Remote File Inclusion
| php/webapps/3[01;31m[K25[m[K9.pl

phpBB-Auction Module 1.0/1.2 - 'Auction_Offer.php' SQL Injection
| php/webapps/[01;31m[K25[m[K475.txt

phpBB-Auction Module 1.0/1.2 - 'Auction_Rating.php' SQL Injection
| php/webapps/[01;31m[K25[m[K474.txt

PHPBB2 Plus 1.5 - 'GroupCP.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K398.txt

PHPBB2 Plus 1.5 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                                  |
php/webapps/[01;31m[K25[m[K399.txt

PHPBB2 Plus 1.5 - 'Portal.php' Multiple Cross-Site Scripting
Vulnerabilities                                 |
php/webapps/[01;31m[K25[m[K400.txt

PHPBB2 Plus 1.5 - 'viewtopic.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K401.txt

phpBBFM 206-3-3 - 'phpbb_root_path' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K64.pl

phpBurningPortal 1.0.1 - 'lang_path' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K63.pl

PHPCart - Input Validation
| php/webapps/[01;31m[K25[m[K548.txt

PHPClassifieds.Info - Multiple Input Validation Vulnerabilities
| php/webapps/281[01;31m[K25[m[K.txt

phpCoin 1.2 - 'auxpage.php?page' Traversal Arbitrary File Access
| php/webapps/[01;31m[K25[m[K302.txt

PHPCOIN 1.2 - 'login.php' Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K175.txt
```

```
phpCOIN 1.2 - 'login.php?PHPcoinsessid' SQL Injection
| php/webapps/[01;31m[K25[m[K568.txt

PHPCOIN 1.2 - 'mod.php' Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K174.txt

phpCOIN 1.2 Pages Module - Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K569.txt

PHPCOIN 1.2.3 - 'session_set.php' Remote File Inclusion
| php/webapps/2[01;31m[K25[m[K4.txt

PhpGedView 2.61 - Search Script Cross-Site Scripting
| php/webapps/235[01;31m[K25[m[K.txt

phpGroupWare 0.9.14 - 'Tables_Update.Inc.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K043.txt

phpGroupWare 0.9.x - 'index.php' HTML Injection
| php/webapps/[01;31m[K25[m[K044.txt

PHPHeaven PHPMyChat 0.14.5 - 'Start-Page.CSS.php3' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K659.txt

PHPHeaven PHPMyChat 0.14.5 - 'Style.CSS.php3' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K660.txt

PHPht Topsites - 'common.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K26.txt

PHPInclude.Worm - PHP Scripts Automated Arbitrary File Inclusion
| php/webapps/7[01;31m[K25[m[K.pl

PHPizabi 0.848b C1 HP3 - 'id' Local File Inclusion
| php/webapps/32[01;31m[K25[m[K1.txt

PHPKB Knowledge Base Software 2.0 - Multilanguage Support Multiple SQL
Injections                          |
php/webapps/1[01;31m[K25[m[K61.txt

PHPLibrary 1.5.3 - 'grid3.lib.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K11.txt

PHPMailer 1.7 - 'Data()' Remote Denial of Service
| php/dos/[01;31m[K25[m[K752.txt

PHPMoAdmin - Unauthorized Remote Code Execution
| php/webapps/36[01;31m[K25[m[K1.txt

phpMyAdmin - 'preg_replace' (Authenticated) Remote Code Execution
(Metasploit)                                |
php/remote/[01;31m[K25[m[K136.rb
```

phpMyAdmin 2.6 - 'display_tbl_links.lib.php' Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/[01;31m[K25[m[K153.txt

phpMyAdmin 2.6 - 'select_server.lib.php' Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/[01;31m[K25[m[K152.txt

phpMyAdmin 2.6 - 'theme_left.css.php' Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/[01;31m[K25[m[K154.txt

phpMyAdmin 2.6 - 'theme_right.css.php' Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/[01;31m[K25[m[K155.txt

phpMyAdmin 2.6 - Multiple Local File Inclusions
| php/webapps/[01;31m[K25[m[K156.txt

phpMyAdmin 2.x - Convcharset Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K330.txt

phpMyAdmin 3.0.1 - 'pmd_pdf.php' Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K31.txt

phpMyAdmin 3.5.8/4.0.0-RC2 - Multiple Vulnerabilities
| php/webapps/[01;31m[K25[m[K003.txt

phpMyAgenda 3.1 - '/templates/header.php3' Local File Inclusion
| php/webapps/[01;31m[K25[m[K00.pl

PHPmybibli 3.0.1 - Multiple Remote File Inclusions
| php/webapps/[01;31m[K25[m[K85.txt

PHPMyConferences 8.0.2 - 'menu.inc.php' File Inclusion
| php/webapps/[01;31m[K25[m[K35.txt

PHPMyDirectory 10.1.3 - 'review.php' Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/[01;31m[K25[m[K276.txt

PHPMyManga 0.8.1 - 'template.php' Multiple File Inclusions
| php/webapps/[01;31m[K25[m[K78.txt

PHPMyVisites 1.3 - 'Set_Lang' File Inclusion
| php/webapps/[01;31m[K25[m[K531.html

PHPMyWind 5.3 - Cross-Site Scripting
| php/webapps/4[01;31m[K25[m[K35.txt

PHPNews 1.2.3/1.2.4 - 'auth.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K180.py

```
PHPOpenChat 2.3.4/3.0.1 - 'ENGLISH_poc.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K229.txt

PHPOpenChat 2.3.4/3.0.1 - 'poc.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K228.txt

PHPOpenChat 2.3.4/3.0.1 - 'poc_loginform.php?phpbb_root_path' Remote
File Inclusion                          |
php/webapps/[01;31m[K25[m[K227.txt

PHPOpenChat 3.0.1 - Multiple HTML Injection Vulnerabilities
| php/webapps/[01;31m[K25[m[K236.html

phpoutsourcing zorum 3.5 - Multiple Vulnerabilities
| php/webapps/[01;31m[K25[m[K206.txt

phpPgAdmin 3.x - Login Form Directory Traversal
| php/webapps/[01;31m[K25[m[K938.txt

PHPPowerCards 2.10 - 'txt.inc.php' Remote Code Execution
| php/webapps/[01;31m[K25[m[K90.txt

PHPRecipeBook 2.35 - 'g_rb_basedir' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K84.pl

phpscripte24 Countdown Standart Rückwärts Auktions System - SQL
Injection                                  |
php/webapps/1[01;31m[K25[m[K35.txt

phpscripte24 Live Shopping Multi Portal System - SQL Injection
| php/webapps/1[01;31m[K25[m[K45.rb

phpscripte24 Shop System - SQL Injection
| php/webapps/1[01;31m[K25[m[K42.rb

PHPsFTPd 0.2/0.4 - 'Inc.login.php' Privilege Escalation
| php/webapps/[01;31m[K25[m[K964.c

PHPSysInfo 2.0/2.3 - 'sensor_program' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K265.txt

PHPSysInfo 2.0/2.3 - 'system_footer.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K266.txt

PhpTax 0.8 - File Manipulation 'newvalue' / Remote Code Execution
| php/webapps/[01;31m[K25[m[K849.txt

phpThumb - 'phpThumbDebug' Information Disclosure
| php/webapps/17[01;31m[K25[m[K0.txt

phpTrafficA 1.4.1 - 'plotStat.php?File' Traversal Local File Inclusion
| php/webapps/296[01;31m[K25[m[K.txt
```

```
PHPWebGallery 1.3.4 - Cross-Site Scripting / Local File Inclusion
| php/webapps/64[01;31m[K25[m[K.txt

phpWebSite 0.10.0-full - 'topics.php' SQL Injection
| php/webapps/15[01;31m[K25[m[K.pl

phpWebSite 0.7.3/0.8.x/0.9.x - 'index.php' Directory Traversal
| php/webapps/[01;31m[K25[m[K945.txt

phpWebSite 0.7.3/0.8.x/0.9.x Comment Module - 'CM_pid' Cross-Site
Scripting                                 |
php/webapps/244[01;31m[K25[m[K.txt

phpWebSite 0.8.2 - PHP File Inclusion
| php/webapps/218[01;31m[K25[m[K.txt

phpWebSite 0.9.3 - 'links.php' SQL Injection
| php/webapps/3[01;31m[K25[m[K53.txt

phpWebSite 0.x - Image File Processing Arbitrary '.PHP' File Upload
| php/webapps/[01;31m[K25[m[K161.txt

PHPWebThings 1.4 - 'forum' SQL Injection
| php/webapps/13[01;31m[K25[m[K.pl

Pi3Web 2.0.1 - GET Denial of Service
| windows/dos/2[01;31m[K25[m[K87.c

Picasm 1.10/1.12 - Error Generation Remote Buffer Overflow
| freebsd/remote/[01;31m[K25[m[K687.c

Pie Web m{a_e}sher mod rss 0.1 - Remote File Inclusion
| php/webapps/72[01;31m[K25[m[K.txt

Pilot Group PG Roommate Finder Solution - SQL Injection
| php/webapps/3[01;31m[K25[m[K97.txt

Pinnacle Cart - 'index.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K394.txt

Pirelli Discus DRG A1[01;31m[K25[m[Kg - Local Password Disclosure
| hardware/webapps/29795.pl

Pirelli Discus DRG A1[01;31m[K25[m[Kg - Password Disclosure
| hardware/webapps/29262.pl

Pirelli Discus DRG A1[01;31m[K25[m[Kg - Remote Change SSID Value
| hardware/webapps/29794.txt

Pirelli Discus DRG A1[01;31m[K25[m[Kg - Remote Change WiFi Password
| hardware/webapps/29796.pl
```

Pirelli Discus DRG A2[01;31m[K25[m[K wifi router - WPA2PSK Default Algorithm |
hardware/remote/8359.py

PivotX 2.2 - '/pivotx/includes/blogroll.php?color' Cross-Site Scripting
| php/webapps/35[01;31m[K25[m[K9.txt

PivotX 2.2.2 - 'module_image.php' Cross-Site Scripting
| php/webapps/35[01;31m[K25[m[K4.txt

Piwigo 2.7.3 - SQL Injection
| php/webapps/361[01;31m[K25[m[K.txt

Pixaria Gallery 2.3.5 - 'file' Remote File Disclosure
| php/webapps/9[01;31m[K25[m[K7.php

Pixie CMS - Cross-Site Scripting / SQL Injection
| php/webapps/8[01;31m[K25[m[K2.txt

Pixie CMS 1.0.4 - '/admin/index.php' SQL Injection
| php/webapps/35[01;31m[K25[m[K1.txt

Plague News System 0.7 - 'CID' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K935.txt

Plague News System 0.7 - 'CID' SQL Injection
| php/webapps/[01;31m[K25[m[K934.txt

Plague News System 0.7 - 'delete.php' Access Restriction Bypass
| php/webapps/[01;31m[K25[m[K937.txt

PlanetDNS PlanetFileServer - Remote Buffer Overflow (PoC)
| windows/dos/[01;31m[K25[m[K936.pl

Plantronics Hub 3.[01;31m[K25[m[K.1 - Arbitrary File Read
| windows/local/52011.txt

PlatinumFTPServer 1.0.18 - Multiple Malformed User Name Connection Denial of Service Vulnerabilities |
windows/dos/[01;31m[K25[m[K218.pl

Plesk < 9.5.4 - Remote Command Execution
| php/remote/[01;31m[K25[m[K986.txt

PMachine Pro 2.4 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K127.txt

PMB 4.1.3 - (Authenticated) SQL Injection
| php/webapps/356[01;31m[K25[m[K.txt

Pngren 2.0.1 - 'Kaiseki.cgi' Remote Command Execution
| cgi/webapps/[01;31m[K25[m[K952.txt

PolyPager 1.0rc10 - 'FCKeditor' Arbitrary File Upload
| php/webapps/1[01;31m[K25[m[K84.txt

Popper Webmail 1.41 - 'ChildWindow.Inc.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K788.txt

Portail Web PHP 2.5.1 - 'includes.php' Remote File Inclusion
| php/webapps/3[01;31m[K25[m[K0.txt

PortailPHP 1.3 - 'ID' SQL Injection
| php/webapps/[01;31m[K25[m[K690.pl

PortalXP Teacher Edition 1.2 - Multiple SQL Injections
| php/webapps/93[01;31m[K25[m[K.txt

Portech MV-372 VoIP Gateway - Multiple Vulnerabilities
| hardware/remote/359[01;31m[K25[m[K.txt

Positive Software H-Sphere Winbox 2.4 - Sensitive Logfile Content
Disclosure |
windows/local/[01;31m[K25[m[K636.txt

Post Comments 3.0 - Insecure Cookie Handling
| php/webapps/66[01;31m[K25[m[K.txt

PostgreSQL 7.x - Multiple Vulnerabilities
| linux/dos/[01;31m[K25[m[K076.c

PostNuke 0.6x/0.7x NS-Languages Module - 'language' Cross-Site
Scripting |
php/webapps/27[01;31m[K25[m[K4.txt

PostNuke 0.6x/0.7x NS-Languages Module - 'language' SQL Injection
| php/webapps/27[01;31m[K25[m[K5.txt

PostNuke 0.75/0.76 Blocks Module - Directory Traversal
| php/webapps/[01;31m[K25[m[K665.txt

PostNuke Phoenix 0.760 RC3 - 'Module' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K367.txt

PostNuke Phoenix 0.760 RC3 - 'OP' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K366.txt

PostNuke Phoenix 0.760 RC3 - 'SID' SQL Injection
| php/webapps/[01;31m[K25[m[K368.txt

PostNuke Phoenix 0.7x - 'CATID' SQL Injection
| php/webapps/[01;31m[K25[m[K172.txt

PostNuke Phoenix 0.7x - 'SHOW' SQL Injection
| php/webapps/[01;31m[K25[m[K173.txt

PotPlayer 1.5.4[01;31m[K25[m[K09 Beta - Integer Division by Zero Denial of Service | windows/dos/30308.py

PowerDownload 3.0.2/3.0.3 - IncDir Remote File Inclusion | php/webapps/[01;31m[K25[m[K777.txt

PPA 0.5.6 - 'ppa_root_path' File Inclusion | php/webapps/[01;31m[K25[m[K960.txt

Pre Jobo .NET - Authentication Bypass | asp/webapps/105[01;31m[K25[m[K.txt

Press Release Script - 'page.php?id' SQL Injection | php/webapps/1[01;31m[K25[m[K97.txt

Primo Place Primo Cart 1.0 - Multiple SQL Injections | php/webapps/270[01;31m[K25[m[K.txt

ProcessMaker Open Source - (Authenticated) PHP Code Execution (Metasploit) | php/remote/293[01;31m[K25[m[K.rb

ProficySCADA for iOS 5.0.[01;31m[K25[m[K920 - 'Password' Denial of Service (PoC) | ios/dos/48236.py

ProfitCode Software PayProCart 3.0 - 'Username' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K488.txt

ProfitCode Software PayProCart 3.0 - 'Usrdetails.php' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K337.txt

ProfitCode Software PayProCart 3.0 - AdminShop HDoc Cross-Site Scripting | php/webapps/[01;31m[K25[m[K490.txt

ProfitCode Software PayProCart 3.0 - AdminShop MMActionComm Cross-Site Scripting | php/webapps/[01;31m[K25[m[K495.txt

ProfitCode Software PayProCart 3.0 - AdminShop ModID Cross-Site Scripting | php/webapps/[01;31m[K25[m[K491.txt

ProfitCode Software PayProCart 3.0 - AdminShop ProMod Cross-Site Scripting | php/webapps/[01;31m[K25[m[K494.txt

ProfitCode Software PayProCart 3.0 - AdminShop TaskID Cross-Site Scripting | php/webapps/[01;31m[K25[m[K492.txt

```
ProfitCode Software PayProCart 3.0 - Ckprvd Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K489.txt

profitcode software payprocart 3.0 - Directory Traversal
| php/webapps/[01;31m[K25[m[K338.txt

ProjectBB 0.4.5.1 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K183.txt

ProjectBB 0.4.5.1 - Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K184.txt

ProManager 0.73 - 'note.php' SQL Injection
| php/webapps/2[01;31m[K25[m[K9.txt

PromoProducts - 'view_product.php' Multiple SQL Injections
| php/webapps/32[01;31m[K25[m[K7.txt

Property Listing Script - 'propid' Blind SQL Injection
| php/webapps/412[01;31m[K25[m[K.txt

ProShow Gold 4.0.[01;31m[K25[m[K49 - '.psh' Local Stack Buffer Overflow
(Metasploit)                                    |
windows/local/16655.rb

ProShow Producer / Gold 4.0.[01;31m[K25[m[K49 - '.psh' Universal Buffer
Overflow (SEH)                                  | windows/local/9519.pl

Prototype of an PHP Application 0.1 -
'/menu/menuprincipal.php?path_inc' Remote File Inclusion            |
php/webapps/301[01;31m[K25[m[K.txt

Proxifier for Mac 2.19 - Local Privilege Escalation
| macos/local/432[01;31m[K25[m[K.sh

Proxomitron Naoko-4 - Cross-Site Scripting
| multiple/remote/210[01;31m[K25[m[K.txt

Prozilla Gaming Directory 1.0 - SQL Injection
| php/webapps/316[01;31m[K25[m[K.txt

PScript PForum 1.24/1.[01;31m[K25[m[K - User Profile HTML Injection
| php/webapps/24373.txt

pserv 3.2 - Directory Traversal
| linux/remote/[01;31m[K25[m[K669.txt

PServ 3.2 - Source Code Disclosure
| cgi/webapps/[01;31m[K25[m[K666.txt

PsNews 1.3 - SQL Injection
| php/webapps/14[01;31m[K25[m[K1.txt
```

PunBB 1.2.3 - Multiple HTML Injection Vulnerabilities
| php/webapps/[01;31m[K25[m[K230.txt

PunBB 1.x - 'profile.php' User Profile Edit Module SQL Injection
| php/webapps/[01;31m[K25[m[K957.txt

PunBB 3.0/3.1 - Multiple Remote Input Validation Vulnerabilities
| php/webapps/[01;31m[K25[m[K160.txt

PWSPHP 1.1/1.2 - 'Profil.php' SQL Injection
| php/webapps/[01;31m[K25[m[K640.txt

PWSPHP 1.2 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K639.txt

PY Software Active Webcam 4.3/5.5 - WebServer Multiple Vulnerabilities
| windows/remote/[01;31m[K25[m[K207.txt

Python - Interpreter Heap Memory Corruption (PoC)
| multiple/dos/33[01;31m[K25[m[K1.txt

Python 2.5.2 - 'Imageop' Module Argument Validation Buffer Overflow
| unix/dos/3[01;31m[K25[m[K34.py

QEMU Guest Agent 2.12.50 - Denial of Service
| linux/dos/449[01;31m[K25[m[K.txt

qEngine CMS 6.0.0 - Multiple Vulnerabilities
| php/webapps/3[01;31m[K25[m[K11.txt

QK SMTP 3.01 - 'RCPT TO' Remote Denial of Service
| windows/dos/26[01;31m[K25[m[K.c

QNAP Transcode Server - Command Execution (Metasploit)
| hardware/remote/4[01;31m[K25[m[K87.rb

QNX PPPoEd 2.4/4.[01;31m[K25[m[K/6.2 - Multiple Local Buffer Overrun
Vulnerabilities |
linux/dos/24569.txt

QNX PPPoEd 2.4/4.[01;31m[K25[m[K/6.2 - Path Environment Variable Local
Command Execution |
linux/local/24570.txt

QNX RTOS 4.[01;31m[K25[m[K - 'CRTTrap' File Disclosure
| linux/local/21499.txt

QNX RTOS 4.[01;31m[K25[m[K - dumper Arbitrary File Modification
| linux/local/21501.txt

QNX RTOS 4.[01;31m[K25[m[K - monitor Arbitrary File Modification
| linux/local/21500.txt

QNX RTOS 4.[01;31m[K25[m[K/6.1 - 'phgrafx' Local Privilege Escalation
| linux/local/21503.sh

QNX RTOS 4.[01;31m[K25[m[K/6.1 - 'phgrafx-startup' Local Privilege
Escalation |
linux/local/21504.sh

QNX RTOS 4.[01;31m[K25[m[K/6.1 - su Password Hash Disclosure
| linux/local/21502.txt

QSSL QNX 4.[01;31m[K25[m[K A - 'crypt()' Local Privilege Escalation
| qnx/local/19851.c

Qualiteam X-Cart 4.0.8 - 'error_message.php?id' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K761.txt

Qualiteam X-Cart 4.0.8 - 'error_message.php?id' SQL Injection
| php/webapps/[01;31m[K25[m[K769.txt

Qualiteam X-Cart 4.0.8 - 'giftcert.php' Multiple Cross-Site Scripting
Vulnerabilities |
php/webapps/[01;31m[K25[m[K766.txt

Qualiteam X-Cart 4.0.8 - 'giftcert.php' Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K774.txt

Qualiteam X-Cart 4.0.8 - 'help.php?section' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K762.txt

Qualiteam X-Cart 4.0.8 - 'help.php?section' SQL Injection
| php/webapps/[01;31m[K25[m[K770.txt

Qualiteam X-Cart 4.0.8 - 'home.php' Multiple Cross-Site Scripting
Vulnerabilities |
php/webapps/[01;31m[K25[m[K759.txt

Qualiteam X-Cart 4.0.8 - 'home.php' Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K767.txt

Qualiteam X-Cart 4.0.8 - 'orders.php?mode' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K763.txt

Qualiteam X-Cart 4.0.8 - 'orders.php?mode' SQL Injection
| php/webapps/[01;31m[K25[m[K771.txt

Qualiteam X-Cart 4.0.8 - 'product.php' Multiple Cross-Site Scripting
Vulnerabilities |
php/webapps/[01;31m[K25[m[K760.txt

Qualiteam X-Cart 4.0.8 - 'product.php' Multiple SQL Injections
| php/webapps/[01;31m[K25[m[K768.txt

```
Qualiteam X-Cart 4.0.8 - 'register.php?mode' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K764.txt

Qualiteam X-Cart 4.0.8 - 'register.php?mode' SQL Injection
| php/webapps/[01;31m[K25[m[K772.txt

Qualiteam X-Cart 4.0.8 - 'search.php?mode' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K765.txt

Qualiteam X-Cart 4.0.8 - 'search.php?mode' SQL Injection
| php/webapps/[01;31m[K25[m[K773.txt

QuantaStor Software Defined Storage < 4.3.1 - Multiple Vulnerabilities
| xml/webapps/4[01;31m[K25[m[K17.txt

Quartz Concept Content Manager 3.00 - Authentication Bypass
| asp/webapps/104[01;31m[K25[m[K.txt

Quick Search 1.1.0.189 - Buffer Overflow (SEH)
| windows/dos/[01;31m[K25[m[K443.txt

Quick.Cart 2.2 - Local/Remote File Inclusion / Remote Code Execution
| php/webapps/40[01;31m[K25[m[K.php

QwikMail 0.3 - 'HELO' Buffer Overflow (PoC)
| linux/dos/[01;31m[K25[m[K004.txt

Racer 0.5.3 Beta 5 - Remote Stack Buffer Overflow
| windows/remote/8[01;31m[K25[m[K3.c

RadioCMS 2.2 - 'menager.php?playlist_id' SQL Injection
| php/webapps/[01;31m[K25[m[K726.txt

RadScripts RadBids Gold 2.0 - 'faq.php?farea' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K371.txt

RadScripts RadBids Gold 2.0 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                    | php/webapps/[01;31m[K25[m[K372.txt

RadScripts RadBids Gold 2.0 - 'index.php?mode' SQL Injection
| php/webapps/[01;31m[K25[m[K370.txt

RadScripts RadBids Gold 2.0 - 'index.php?read' Traversal Arbitrary File
Access                             | php/webapps/[01;31m[K25[m[K369.txt

RahnemaCo - 'page.php' Remote File Inclusion
| php/webapps/280[01;31m[K25[m[K.txt

RaidenFTPd 2.4 - Unauthorized File Access
| windows/remote/[01;31m[K25[m[K486.txt

RaidenHTTPD 1.1.27 - Remote File Disclosure
| windows/dos/[01;31m[K25[m[K083.txt
```

```
RakhiSoftware Shopping Cart - SQL Injection
| php/webapps/7[01;31m[K25[m[K0.txt

Rakkarsoft RakNet 2.33 - Remote Denial of Service
| multiple/dos/[01;31m[K25[m[K791.txt

Raven Software Soldier Of Fortune 2 - Ignore Command Remote Denial of
Service                                 |
windows/dos/[01;31m[K25[m[K921.txt

RaXnet Cacti 0.5/0.6.x/0.8.x - 'Graph_Image.php' Remote Command
Execution Variant                       |
php/webapps/[01;31m[K25[m[K927.pl

RaXnet Cacti 0.5/0.6/0.8 - 'Config_Settings.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K857.txt

RaXnet Cacti 0.5/0.6/0.8 - 'Top_Graph_Header.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K859.txt

RCA DCM4[01;31m[K25[m[K Cable Modem - 'micro_httpd' Denial of Service
(PoC)                                                   |
hardware/dos/11597.py

RealAdmin - 'detail.php' Blind SQL Injection
| php/webapps/113[01;31m[K25[m[K.txt

RealityServer Web Services RTMP Server 3.1.1 build
1445[01;31m[K25[m[K.5 - Null Pointer Dereference Denial of Service   |
windows/dos/35895.txt

realnetworks realarcade 1.2.0.994 - Multiple Vulnerabilities
| multiple/remote/[01;31m[K25[m[K091.txt

Redaction System 1.0 - 'lang_prefix' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K34.pl

REDDOXX Appliance Build 2032 / 2.0.6[01;31m[K25[m[K - Arbitrary File
Disclosure                                              |
json/webapps/42372.txt

REDDOXX Appliance Build 2032 / 2.0.6[01;31m[K25[m[K - Remote Command
Execution                                               |
json/webapps/42371.txt

RedHat 6.1 - 'man' Local Overflow / Local Privilege Escalation
| linux/local/[01;31m[K25[m[K5.pl

RedHat Linux 5.2 i386/6.0 - No Logging
| linux/local/19[01;31m[K25[m[K5.txt

registroTL - 'main.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K02.txt
```

```
reiserfstune 3.6.[01;31m[K25[m[K - Local Buffer Overflow
| linux/dos/42110.txt

Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)
| windows/webapps/491[01;31m[K25[m[K.py

Remote Mouse 4.002 - Unquoted Service Path
| windows/local/50[01;31m[K25[m[K8.txt

Remote Utilities Host 6.3 - Denial of Service
| windows/dos/408[01;31m[K25[m[K.py

Remotesoft .NET Explorer 2.0.1 - Local Stack Overflow (PoC)
| windows/dos/3[01;31m[K25[m[K4.py

Responsive FileManager 9.9.5 - Remote Code Execution (RCE)
| php/webapps/51[01;31m[K25[m[K1.py

Revou Twitter Clone - Cross-Site Scripting / SQL Injection
| php/webapps/79[01;31m[K25[m[K.txt

REZERVI 3.0.2 - Remote Command Execution
| php/webapps/1[01;31m[K25[m[K23.py

RPi Cam Control < 6.4.[01;31m[K25[m[K - 'preview.php' Remote Command
Execution                                              |
linux/webapps/45361.py

RSA Security RSA Authentication Agent For Web 5.2 - Cross-Site
Scripting                                        |
windows/remote/[01;31m[K25[m[K421.txt

RTF2LATEX2E 1.0 - Remote Stack Buffer Overflow
| linux/remote/[01;31m[K25[m[K006.txt

RUMBA 7.3/7.4 - Profile Handling Multiple Buffer Overflow
Vulnerabilities                                    |
windows/dos/[01;31m[K25[m[K326.txt

Rumble 0.[01;31m[K25[m[K.2232 - Denial of Service
| windows/dos/17070.py

Rumble Mail Server 0.51.3135 - 'domain and path' Stored XSS
| multiple/webapps/49[01;31m[K25[m[K4.txt

Rumble Mail Server 0.51.3135 - 'servername' Stored XSS
| multiple/webapps/49[01;31m[K25[m[K3.txt

Rumble Mail Server 0.51.3135 - 'username' Stored XSS
| multiple/webapps/49[01;31m[K25[m[K5.txt

RunCMS 1.1 - Database Configuration Information Disclosure
| php/webapps/[01;31m[K25[m[K237.txt
```

```
RunCMS 1.6.1 - 'admin.php' Cross-Site Scripting
| php/webapps/312[01;31m[K25[m[K.html

RunCMS 1.x - 'Ratefile.php' Cross-Site Scripting
| php/webapps/27[01;31m[K25[m[K6.txt

Rundeck Community Edition < 3.0.13 - Persistent Cross-Site Scripting
| java/webapps/46[01;31m[K25[m[K1.txt

Ruubikcms 1.1.1 - 'tinybrowser.php?folder' Directory Traversal
| php/webapps/[01;31m[K25[m[K973.txt

Ruubikcms 1.1.1 - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K996.txt

S.u.S.E Linux 5.2 - 'gnuplot' Local Overflow / Local Privilege
Escalation                                  |
linux/local/19[01;31m[K25[m[K4.c

S.u.S.E Linux 5.2 - 'lpc' Local Privilege Escalation
| linux/local/19[01;31m[K25[m[K9.c

Salim Gasmi GLD (Greylisting Daemon) 1.x - Postfix Greylisting Daemon
Buffer Overflow                       |
linux/remote/[01;31m[K25[m[K392.c

Samba 3.0.20 < 3.0.[01;31m[K25[m[Krc3 - 'Username' map script' Command
Execution (Metasploit)                             | unix/remote/16320.rb

Samba 3.4.7/3.5.1 - Denial of Service
| linux/dos/1[01;31m[K25[m[K88.txt

Sambar Server 5.x/6.0/6.1 - 'results.stm' indexname Cross-Site
Scripting                                   |
windows/remote/[01;31m[K25[m[K694.txt

Sambar Server 5.x/6.0/6.1 - logout RCredirect Cross-Site Scripting
| windows/remote/[01;31m[K25[m[K695.txt

Sambar Server 5.x/6.0/6.1 - Server Referer Cross-Site Scripting
| windows/remote/[01;31m[K25[m[K696.txt

Samsung Galaxy S6 - 'android.media.process' 'MdConvertLine' Face
Recognition Memory Corruption             |
android/dos/394[01;31m[K25[m[K.txt

sandbox 2.0.3 - Multiple Vulnerabilities
| php/webapps/14[01;31m[K25[m[K5.txt

SAP Database 7.3/7.4 - SDBINST Race Condition
| linux/local/2[01;31m[K25[m[K31.pl
```

SAP Internet Transaction Server 6.10/6.20 - Cross-Site Scripting
| multiple/remote/287[01;31m[K25[m[K.txt

SAP SOAP RFC - SXPG_CALL_SYSTEM Remote Command Execution (Metasploit)
| multiple/remote/[01;31m[K25[m[K445.rb

SAP SOAP RFC - SXPG_COMMAND_EXECUTE Remote Command Execution
(Metasploit) |
multiple/remote/[01;31m[K25[m[K446.rb

SAS Integration Technologies Client 9.31_M1 'SASspk.dll' - Stack
Overflow |
windows/dos/[01;31m[K25[m[K714.txt

Savsoft Quiz 5 - 'User Account Settings' Persistent Cross-Site
Scripting |
php/webapps/498[01;31m[K25[m[K.txt

School Attendance Monitoring System 1.0 - Cross-Site Request Forgery
(Update Admin) |
php/webapps/457[01;31m[K25[m[K.txt

Schools Alert Management Script - Authentication Bypass
| php/webapps/4[01;31m[K25[m[K78.txt

SCO OpenServer 5.0.6/5.0.7 - NWPrint Command Line Argument Local Buffer
Overflow | unix/local/[01;31m[K25[m[K333.c

Scripteen Free Image Hosting Script 2.3 - Insecure Cookie Handling
| php/webapps/9[01;31m[K25[m[K6.txt

Scripteen Free Image Hosting Script 2.3 - SQL Injection
| php/webapps/9[01;31m[K25[m[K2.txt

sd server 4.0.70 - Directory Traversal
| windows/remote/[01;31m[K25[m[K144.txt

Seacms 11.1 - 'checkuser' Stored XSS
| multiple/webapps/49[01;31m[K25[m[K1.txt

Seacms 11.1 - 'file' Local File Inclusion
| multiple/webapps/49[01;31m[K25[m[K0.txt

Seagate BlackArmor NAS sg2000-2000.1331 - Remote Command Execution
| hardware/webapps/307[01;31m[K25[m[K.txt

See-Commerce 1.0.6[01;31m[K25[m[K - 'owimg.php3' Remote File Inclusion
| php/webapps/2155.txt

SEO Panel 4.6.0 - Remote Code Execution (2)
| php/webapps/495[01;31m[K25[m[K.py

Seowonintech Routers fw: 2.3.9 - File Disclosure
| hardware/webapps/[01;31m[K25[m[K968.pl

Serva 32 TFTP 2.1.0 - Buffer Overflow (Denial of Service) (PoC)
| windows/dos/[01;31m[K25[m[K472.py

ServersCheck 5.9/5.10 - Directory Traversal
| windows/remote/[01;31m[K25[m[K755.txt

Seyon 2.1 rev. 4b i586-Linux (RedHat 4.0/5.1) - Local Overflow
| linux/local/[01;31m[K25[m[K2.pl

SGI IRIX 6.5.22 - GR_OSView Information Disclosure
| irix/local/[01;31m[K25[m[K361.txt

SGI IRIX 6.5.22 - GR_OSView Local Arbitrary File Overwrite
| irix/local/[01;31m[K25[m[K362.txt

SH-News 3.1 - 'scriptpath' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K18.txt

ShareCMS 0.1 - Multiple SQL Injections
| php/webapps/59[01;31m[K25[m[K.txt

Shop-Script - categoryId SQL Injection
| php/webapps/[01;31m[K25[m[K663.txt

Shop-Script - ProductID SQL Injection
| php/webapps/[01;31m[K25[m[K664.txt

ShopCartDx 4.30 - 'products.php' Blind SQL Injection
| php/webapps/141[01;31m[K25[m[K.pl

Shopware 3.5 - SQL Injection
| php/webapps/198[01;31m[K25[m[K.php

showoff! digital media software 1.5.4 - Multiple Vulnerabilities
| cgi/webapps/[01;31m[K25[m[K649.txt

Sielco Sistemi Winlog 2.07.14 - Remote Buffer Overflow (Metasploit)
| windows/remote/190[01;31m[K25[m[K.rb

SIEMENS IP Camera CCMW10[01;31m[K25[m[K x.2.2.1798 - Remote Admin
Credentials Change |
cgi/webapps/40260.sh

SIEMENS IP-Camera CVMS20[01;31m[K25[m[K-IR / CCMS20[01;31m[K25[m[K -
Credentials Disclosure |
cgi/webapps/40[01;31m[K25[m[K4.txt

Siemens SIPROTEC 4 and SIPROTEC Compact EN100 Ethernet Module <
4.[01;31m[K25[m[K - Denial of Service |
hardware/dos/44103.py

SIEMENS Solid Edge ST4/ST5 SEListCtrlX - ActiveX SetItemReadOnly Arbitrary Memory Rewrite Remote Code Exec | windows/dos/[01;31m[K25[m[K712.txt

SIEMENS Solid Edge ST4/ST5 WebPartHelper - ActiveX RFMSsvs!JShellExecuteEx Remote Code Execution | windows/remote/[01;31m[K25[m[K713.txt

Sigma ISP Manager 6.6 - 'Sigmaweb.dll' SQL Injection | cgi/webapps/[01;31m[K25[m[K668.txt

Silly Poker 0.[01;31m[K25[m[K.5 - Local HOME Environment Variable Buffer Overrun | linux/local/23204.c

SilverPlatter WebSPIRS 3.3.1 - File Disclosure | multiple/remote/206[01;31m[K25[m[K.txt

SimpGB 1.0 - 'Guestbook.php' SQL Injection | php/webapps/[01;31m[K25[m[K224.txt

Simple Invoices 2007 05 [01;31m[K25[m[K - 'index.php?submit' SQL Injection | php/webapps/4098.php

Simple Message Board 2.0 beta1 - 'Forum.cfm' Cross-Site Scripting | cfm/webapps/[01;31m[K25[m[K982.txt

Simple Message Board 2.0 beta1 - 'Search.cfm' Cross-Site Scripting | cfm/webapps/[01;31m[K25[m[K985.txt

Simple Message Board 2.0 beta1 - 'Thread.cfm' Cross-Site Scripting | cfm/webapps/[01;31m[K25[m[K984.txt

Simple Message Board 2.0 beta1 - 'User.cfm' Cross-Site Scripting | cfm/webapps/[01;31m[K25[m[K983.txt

simplecam 1.2 - Directory Traversal | windows/remote/[01;31m[K25[m[K600.txt

SimpleTransfer 2.2.1 - Command Injection | hardware/webapps/[01;31m[K25[m[K416.txt

Simplog 0.9.3.1 - 'comments.php' SQL Injection | php/webapps/[01;31m[K25[m[K74.php

SimplyShare 1.4 iOS - Multiple Vulnerabilities | ios/webapps/31[01;31m[K25[m[K8.txt

Singapore 0.9.11 Beta Image Gallery - 'index.php' Cross-Site Scripting | php/webapps/[01;31m[K25[m[K818.txt

```
Sitecom MD-[01;31m[K25[m[Kx - Multiple Vulnerabilities
| hardware/remote/21268.py

Sitecom WLM-[01;31m[K25[m[K01 - Cross-Site Request Forgery
| hardware/webapps/18597.txt

Sitecom WLM-[01;31m[K25[m[K01 - Multiple Cross-Site Request Forgery
Vulnerabilities                                    |
asp/webapps/18651.txt

SiteEnable - SQL Injection
| asp/webapps/[01;31m[K25[m[K332.txt

Siteman 1.1 - User Database Privilege Escalation (1)
| php/webapps/[01;31m[K25[m[K052.pl

Siteman 1.1 - User Database Privilege Escalation (2)
| php/webapps/[01;31m[K25[m[K053.html

SitePanel2 2.6.1 - Multiple Input Validation Vulnerabilities
| php/webapps/[01;31m[K25[m[K591.txt

SiteWare 2.5/3.0/3.1 Editor Desktop - Directory Traversal
| java/webapps/209[01;31m[K25[m[K.txt

Skeletonz CMS - Persistent Cross-Site Scripting
| cgi/webapps/156[01;31m[K25[m[K.txt

Skull-Splitter Guestbook 1.0/2.0/2.2 - Multiple HTML Injection
Vulnerabilities                                |
php/webapps/[01;31m[K25[m[K662.txt

Skype Technologies Skype 0.92/1.0/1.1 - Insecure Temporary File
Creation                                       |
linux/local/[01;31m[K25[m[K993.sh

SkypeApp 12.8.487.0 - 'Cuenta de Skype o Microsoft' Denial of Service
(PoC)                                  | windows_x86-
64/dos/45[01;31m[K25[m[K1.py

sleuthkit 4.11.1 - Command Injection
| multiple/local/512[01;31m[K25[m[K.txt

Slooze PHP Web Photo Album 0.2.7 - Command Execution
| php/webapps/1[01;31m[K25[m[K15.txt

Smail 3 - Multiple Remote/Local Vulnerabilities
| linux/remote/[01;31m[K25[m[K275.c

Smart Chat 1.0.0 - SQL Injection
| php/webapps/4[01;31m[K25[m[K69.txt
```

Smart Search 4.[01;31m[K25[m[K - Remote Command Execution
| cgi/webapps/22380.pl

SmartCMS 2 - SQL Injection
| php/webapps/1[01;31m[K25[m[K07.txt

SmarterMail < 7.2.39[01;31m[K25[m[K - LDAP Injection
| asp/webapps/15189.txt

SmarterMail < 7.2.39[01;31m[K25[m[K - Persistent Cross-Site Scripting
| asp/webapps/15185.txt

smeweb 1.4b - SQL Injection / Cross-Site Scripting
| php/webapps/57[01;31m[K25[m[K.txt

SnapProof - 'page.php' SQL Injection
| php/webapps/16[01;31m[K25[m[K7.txt

Snitz Forums 2000 - 'register.asp' SQL Injection
| asp/webapps/2[01;31m[K25[m[K83.pl

Snort 2.1/2.2 - DecodeTCPOptions Remote Denial of Service (1)
| linux/dos/[01;31m[K25[m[K046.c

Snort 2.1/2.2 - DecodeTCPOptions Remote Denial of Service (2)
| linux/dos/[01;31m[K25[m[K047.c

Snort 2.x - PrintTcpOptions Remote Denial of Service
| linux/dos/26[01;31m[K25[m[K1.c

Social Site Generator 2.2 - Cross-Site Request Forgery (Add Admin)
| php/webapps/[01;31m[K25[m[K245.txt

SocialABC NetworX 1.0.3 - Arbitrary File Upload / Cross-Site Scripting
| php/webapps/34[01;31m[K25[m[K6.py

Softbiz Classifieds Script - Cross-Site Scripting
| php/webapps/3[01;31m[K25[m[K95.txt

Softerra PHP Developer Library 1.5.3 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K20.txt

SoftiaCom wMailServer 1.0 - Local Information Disclosure
| windows/local/[01;31m[K25[m[K961.c

Softros Network Time System Server 2.3.4 - Denial of Service
| windows/dos/44[01;31m[K25[m[K5.txt

software602 602 lan suite 2004 - Directory Traversal
| windows/remote/[01;31m[K25[m[K621.txt

Software602 602 Lan Suite 2004 2004.0.04.1221 - Arbitrary File Upload
| windows/remote/[01;31m[K25[m[K092.txt

Softwin BitDefender - AvxScanOnlineCtrl COM Object Information Disclosure | windows/remote/240[01;31m[K25[m[K.txt

Solaris - RSH Stack Clash Privilege Escalation (Metasploit) | solaris/local/456[01;31m[K25[m[K.rb

Solaris 10 libnspr - 'LD_PRELOAD' Arbitrary File Creation Privilege Escalation (1) | solaris/local/[01;31m[K25[m[K43.sh

Solaris 10 libnspr - 'LD_PRELOAD' Arbitrary File Creation Privilege Escalation (2) | solaris/local/[01;31m[K25[m[K69.sh

Solaris 2.6/2.7 - '/usr/bin/write' Local Overflow | solaris/local/[01;31m[K25[m[K6.c

Solaris 7/8-beta - ARP Local Overflow | solaris/local/[01;31m[K25[m[K0.c

SonicWALL - Content Filtering Blocked Site Error Page Cross-Site Scripting | hardware/remote/3[01;31m[K25[m[K52.txt

SonicWall NSA 6600/5600/4600/3600/2600/[01;31m[K25[m[K0M - Multiple Vulnerabilities | hardware/webapps/43459.txt

SonicWALL SOHO 5.1.7 - Web Interface Multiple Remote Input Validation Vulnerabilities | cgi/webapps/[01;31m[K25[m[K331.txt

Sony Bravia KDL-32CX5[01;31m[K25[m[K - 'hping' Remote Denial of Service | multiple/dos/37061.txt

Sony Ericsson P900 Beamer - Malformed File Name Handling Denial of Service | hardware/dos/[01;31m[K25[m[K711.txt

Sony Playstation 3 (PS3) 4.31 - Save Game Preview '.SFO' Handling Local Command Execution | hardware/local/[01;31m[K25[m[K718.txt

Sophos Cyberoam UTM CR[01;31m[K25[m[KiNG - 10.6.3 MR-5 - Direct Object Reference | jsp/webapps/44469.txt

Sophos Products - Multiple Vulnerabilities | multiple/remote/2[01;31m[K25[m[K09.txt

Sophos Web Appliance 4.2.1.3 - Remote Code Execution | php/webapps/407[01;31m[K25[m[K.txt

Sorinara Streaming Audio Player 0.9 - '.pla' Local Stack Overflow (PoC)
| windows/dos/86[01;31m[K25[m[K.pl

SOUND4 LinkAndShare Transmitter 1.1.2 - Format String Stack Buffer
Overflow |
hardware/remote/51[01;31m[K25[m[K9.txt

Spaceacre - Multiple SQL Injections
| php/webapps/1[01;31m[K25[m[K51.txt

Specimen Image Database - 'client.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K76.txt

SPHPBlog 0.4 - 'search.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K423.txt

SpiceWorks 7.5 TFTP - Remote File Overwrite / Upload
| windows/remote/418[01;31m[K25[m[K.txt

Spid 1.3 - 'lang_path' File Inclusion
| php/webapps/[01;31m[K25[m[K959.txt

Spinworks Application Server 3.0 - Remote Denial of Service
| windows/dos/[01;31m[K25[m[K219.txt

SPIP CMS < 2.0.23/ 2.1.22/3.0.9 - Privilege Escalation
| php/webapps/334[01;31m[K25[m[K.py

SpitFire Photo Pro - 'pages.php' SQL Injection
| php/webapps/3[01;31m[K25[m[K54.txt

Spread The Word - Multiple Cross-Site Scripting Vulnerabilities
| asp/webapps/[01;31m[K25[m[K700.txt

Spread The Word - Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K701.txt

Spy Emergency [01;31m[K25[m[K.0.650 - 'Multiple' Unquoted Service Path
| windows/local/49997.txt

SqWebMail 3.x/4.0 - HTTP Response Splitting
| php/webapps/[01;31m[K25[m[K534.txt

Stadtaus.Com Download Center Lite 1.5 - PHP Remote File Inclusion
| php/webapps/[01;31m[K25[m[K189.txt

Stadtaus.Com PHP Form Mail Script 2.3 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K192.pl

StageTracker 2.5 - Denial of Service
| windows/dos/159[01;31m[K25[m[K.txt

```
Stanford University bootpd 2.4.3 / Debian 2.0 - netstd
| linux/local/19[01;31m[K25[m[K6.c

Star Articles 6.0 - Arbitrary File Upload
| php/webapps/7[01;31m[K25[m[K1.txt

Star Wars Jedi Knight: Jedi Academy 1.0.11 - Buffer Overflow (PoC)
| windows/dos/[01;31m[K25[m[K329.cfg

Status2k - Remote Add Admin
| php/webapps/11[01;31m[K25[m[K8.html

Stock Management System 1.0 - 'Categories Name' Persistent Cross-Site
Scripting                              |
php/webapps/489[01;31m[K25[m[K.txt

Stockman Shopping Cart 7.8 - Arbitrary Command Execution
| cgi/webapps/2[01;31m[K25[m[K59.pl

StorePortal 2.63 - 'default.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K529.txt

Stormy Studios KNet 1.x - Remote Buffer Overflow
| multiple/dos/[01;31m[K25[m[K165.c

Streamripper 1.61.[01;31m[K25[m[K - HTTP Header Parsing Buffer Overflow
(1)                                            | linux/remote/2274.c

Streamripper 1.61.[01;31m[K25[m[K - HTTP Header Parsing Buffer Overflow
(2)                                            | windows/remote/2277.c

Struts 2.0.11 - Multiple Directory Traversal Vulnerabilities
| multiple/remote/3[01;31m[K25[m[K65.txt

StyleWriter 4 1.0 - Denial of Service (PoC)
| windows_x86/dos/45[01;31m[K25[m[K0.py

Subdreamer 1.0 - SQL Injection
| php/webapps/[01;31m[K25[m[K235.txt

Subrion 3.x - Multiple Vulnerabilities
| php/webapps/385[01;31m[K25[m[K.txt

Subscribe Me Pro 2.44 - S.pl Directory Traversal
| php/webapps/26[01;31m[K25[m[K2.txt

Subtitle Processor 7.7.1 - '.m3u' File Buffer Overflow (SEH Unicode)
(Metasploit)                           |
windows/local/172[01;31m[K25[m[K.rb

SudBox Boutique 1.2 - 'login.php' Authentication Bypass
| php/webapps/226[01;31m[K25[m[K.txt
```

```
sudo 1.8.0 < 1.8.3p1 - 'sudo_debug' glibc FORTIFY_SOURCE Bypass +
Privilege Escalation                    |
linux/local/[01;31m[K25[m[K134.c

Sudo 1.8.[01;31m[K25[m[Kp - 'pwfeedback' Buffer Overflow
| linux/local/48052.sh

Sudo 1.8.[01;31m[K25[m[Kp - 'pwfeedback' Buffer Overflow (PoC)
| linux/dos/47995.txt

Sun Java System Identity Manager 6.0/7.x - Multiple Vulnerabilities
| jsp/webapps/3[01;31m[K25[m[K79.html

Sun Java Virtual Machine 1.2.2/1.3.1 - Segmentation Violation
| linux/local/21[01;31m[K25[m[K9.java

Sun Java Web Start 1.0/1.2 - Remote Command Execution
| multiple/remote/3[01;31m[K25[m[K29.java

Sun JavaMail 1.3 - API MimeMessage Infromation Disclosure
| jsp/webapps/[01;31m[K25[m[K685.txt

Sun JavaMail 1.3.2 - 'MimeBodyPart.getFileName' Directory Traversal
| multiple/remote/[01;31m[K25[m[K395.txt

Sun JavaMail 1.x - Multiple Information Disclosure Vulnerabilities
| java/webapps/[01;31m[K25[m[K702.txt

Sun Solaris 10 Traceroute - Multiple Local Buffer Overflow
Vulnerabilities                                 |
solaris/local/[01;31m[K25[m[K896.pl

Sun Solaris 7.0 - 'ff.core' Local Privilege Escalation
| solaris/local/19[01;31m[K25[m[K8.sh

Sun Solaris 8/9 UCB/PS - Command Local Information Disclosure
| solaris/local/284[01;31m[K25[m[K.txt

Sun Solaris sadmind - 'adm_build_path()' Remote Buffer Overflow
(Metasploit)                            |
solaris/remote/163[01;31m[K25[m[K.rb

SunOS 5.10 Sun Cluster - 'rpc.metad' Denial of Service (PoC)
| solaris/dos/5[01;31m[K25[m[K8.c

Supernews 1.5 - 'valor.php?noticia' SQL Injection
| php/webapps/8[01;31m[K25[m[K5.txt

SurfControl SuperScout Email Filter 3.5 - User Credential Disclosure
| asp/webapps/219[01;31m[K25[m[K.txt

SurgeLDAP 1.0 d - 'User.cgi' Cross-Site Scripting
| cgi/webapps/230[01;31m[K25[m[K.txt
```

```
Surreal ToDo 0.6.1.2 - SQL Injection
| php/webapps/458[01;31m[K25[m[K.txt

SwiFTP 1.11 - Overflow (Denial of Service) (PoC)
| hardware/dos/111[01;31m[K25[m[K.pl

Symantec Altiris Client Service 6.8.378 - Local Privilege Escalation
| windows/local/56[01;31m[K25[m[K.c

Symantec Brightmail Anti-Spam 6.0 - Unauthorized Message Disclosure
| cgi/webapps/24[01;31m[K25[m[K1.txt

Symantec Endpoint Protection 12.1.4013 - Service Disabling
| windows/dos/375[01;31m[K25[m[K.txt

Symantec Messaging Gateway 10.6.2-7 - Remote Code Execution
(Metasploit)                                    |
python/remote/42[01;31m[K25[m[K1.rb

Symantec Messaging Gateway 10.6.3-2 - Root Remote Command Execution
| jsp/webapps/4[01;31m[K25[m[K19.txt

Sync Breeze Enterprise 9.9.16 - Remote Buffer Overflow (SEH)
| windows/remote/4[01;31m[K25[m[K59.py

SyncBreeze 10.1.16 - XML Parsing Stack-based Buffer Overflow
| windows/webapps/497[01;31m[K25[m[K.py

SyncBreeze 15.2.24 - 'login' Denial of Service
| windows/dos/517[01;31m[K25[m[K.py

SysAid Help Desk Software 14.4.32 b[01;31m[K25[m[K - SQL Injection
(Metasploit)                                              |
windows/webapps/38822.rb

Sysax Multi Server 4.3 - Arbitrary Delete Files Expoit
| windows/remote/8[01;31m[K25[m[K6.c

Sysax Multi Server < 5.[01;31m[K25[m[K (SFTP Module) - Multiple Denial
of Service Vulnerabilities                          |
windows/dos/13958.txt

Syslog LogAnalyzer 3.6.5 - Persistent Cross-Site Scripting
| multiple/webapps/345[01;31m[K25[m[K.txt

Syslog Watcher Pro 2.8.0.812 - 'Date' Cross-Site Scripting
| windows/dos/[01;31m[K25[m[K135.txt

Tadbir CMS - 'FCKeditor' Arbitrary File Upload
| php/webapps/1[01;31m[K25[m[K56.txt

Tandis CMS 2.5 - 'index.php' Multiple SQL Injections
| php/webapps/3[01;31m[K25[m[K33.txt
```

```
Task Management System 1.0 - 'page' Local File Inclusion
| php/webapps/49[01;31m[K25[m[K8.txt

tcpdump 3.4 - Protocol Four / Zero Header Length
| linux/remote/19[01;31m[K25[m[K1.c

TeamSpeak 3.0.0-beta[01;31m[K25[m[K - Multiple Vulnerabilities
| windows/dos/13959.txt

TeamSpeak Server 2.0.23 (Multiple Scripts) - Multiple Cross-Site
Scripting Vulnerabilities                 |
multiple/remote/300[01;31m[K25[m[K.txt

Techland XPand Rally 1.0/1.1 - Remote Format String
| multiple/remote/[01;31m[K25[m[K205.txt

tekno.Portal 0.1b - 'makale.php?id' SQL Injection
| php/webapps/1[01;31m[K25[m[K52.txt

Telekorn Signkorn Guestbook 1.x - '/includes/admin.inc.php?dir_path'
Remote File Inclusion                 |
php/webapps/285[01;31m[K25[m[K.txt

Template Seller Pro 3.[01;31m[K25[m[K - 'tempid' SQL Injection
| php/webapps/12360.pl

Tenda AC15 Router - Remote Code Execution
| hardware/remote/44[01;31m[K25[m[K3.py

tForum b0.9 - 'member.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K997.txt

TFTPD32 2.50 - 'Filename' Remote Buffer Overflow
| windows/remote/220[01;31m[K25[m[K.pl

TFTPGUI 1.4.5 - Long Transport Mode Overflow Denial of Service
(Metasploit)                                |
windows/dos/1[01;31m[K25[m[K30.rb

The Includer 1.0/1.1 - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K314.txt

The Shop v2.5 - SQL Injection
| php/webapps/515[01;31m[K25[m[K.txt

thEngine 0.1 - Local File Inclusion
| php/webapps/1[01;31m[K25[m[K04.txt

ThisIsWhyImBroke Clone Script 4.0 - 'id' SQL Injection
| php/webapps/41[01;31m[K25[m[K3.txt

Thomson TCW690 Cable Modem ST42.03.0a - GET Denial of Service
| hardware/dos/[01;31m[K25[m[K124.txt
```

TikiWiki 1.9.8 - 'tiki-graph_formula.php' Command Execution
| php/webapps/45[01;31m[K25[m[K.pl

Tincat Network Library - Remote Buffer Overflow
| multiple/remote/[01;31m[K25[m[K291.txt

TinyIdentD 2.2 - Remote Buffer Overflow
| windows/remote/39[01;31m[K25[m[K.py

Tkai's Shoutbox - 'Query' Open Redirection
| php/webapps/[01;31m[K25[m[K299.txt

Tlen.pl 5.23.4.1 - Instant Messenger Remote Script Execution
| cgi/webapps/[01;31m[K25[m[K042.txt

Tomabo MP4 Converter 3.[01;31m[K25[m[K.22 - Denial of Service (PoC)
| windows/dos/46848.py

Topic Calendar 1.0.1 - 'Calendar_Scheduler.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K270.txt

TORCS 1.3.1 - acc Buffer Overflow
| windows/local/18[01;31m[K25[m[K8.c

TornadoStore 1.4.3 - SQL Injection / HTML Injection
| php/webapps/342[01;31m[K25[m[K.txt

TortoiseSVN 1.12.1 - Remote Code Execution
| windows/webapps/47[01;31m[K25[m[K2.txt

TP-Link Archer C50 3 - Denial of Service (PoC)
| hardware/dos/48[01;31m[K25[m[K5.py

TP-Link IP Cameras Firmware 1.6.18P12 - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K25[m[K812.txt

TP-Link TL-WR[01;31m[K25[m[K43ND Router - Admin Panel Multiple Cross-Site Request Forgery Vulnerabilities |
hardware/remote/38308.txt

TP-Link TL-WR740N v4 Router (FW-Ver. 3.16.6 Build 130529 Rel.47286n) - Command Execution |
hardware/webapps/34[01;31m[K25[m[K4.txt

TP-Link VN020 F3v(T) TT_V6.2.1021 - Denial Of Service (DOS)
| multiple/remote/52[01;31m[K25[m[K0.txt

TP-Link WR842ND - Remote Multiple SSID Directory Traversals
| hardware/webapps/[01;31m[K25[m[K810.py

TrackerCam 5.12 - 'ComGetLogFile.php3?fm' Traversal Arbitrary File Access |
php/webapps/[01;31m[K25[m[K123.txt

Tree Studio 2.17 - Denial of Service (PoC)
| windows/dos/461[01;31m[K25[m[K.py

Trend Micro DirectPass 1.5.0.1060 - Multiple Software Vulnerabilities
| windows/dos/[01;31m[K25[m[K719.txt

Trend Micro Interscan VirusWall for Windows NT 3.52 - Space Gap Scan Bypass |
windows/remote/216[01;31m[K25[m[K.pl

Trend Micro IWSS 3.1 - Local Privilege Escalation
| linux/local/36[01;31m[K25[m[K7.txt

Trend Micro ScanMail for Domino 2.51/2.6 - Remote File Disclosure
| multiple/remote/247[01;31m[K25[m[K.php

TRG News 3.0 Script - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K243.txt

TribunaLibre 3.12 Beta - 'ftag.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K01.txt

Trillian 0.7[01;31m[K25[m[K/0.73/0.74 - IRC User Mode Numeric Remote Buffer Overflow |
windows/dos/21816.c

Tru64 5 - 'su' Env Local Stack Overflow
| tru64/local/[01;31m[K25[m[K9.c

Tru64 UNIX 5.0 (Rev. 910) - edauth NLSPATH Buffer Overflow
| tru64/local/16[01;31m[K25[m[K.pl

Truegalerie 1.0 - Unauthorized Administrative Access
| php/webapps/2[01;31m[K25[m[K34.txt

ttCMS 2.2 / ttForum 1.1 - 'install.php?installdir' Remote File Inclusion |
php/webapps/2[01;31m[K25[m[K78.txt

ttCMS 2.2 / ttForum 1.1 - 'news.php?template' Remote File Inclusion
| php/webapps/2[01;31m[K25[m[K77.txt

TTS Software Time Tracking Software 3.0 - 'edituser.php' Access Validation |
php/webapps/27[01;31m[K25[m[K0.txt

Turnkey Arcade Script - SQL Injection (1)
| php/webapps/7[01;31m[K25[m[K6.txt

TurnkeyForms Software Directory 1.0 - SQL Injection / Cross-Site Scripting |
php/webapps/3[01;31m[K25[m[K71.txt

```
TVMOBiLi 2.1.0.3557 - Denial of Service
| windows/dos/23[01;31m[K25[m[K4.txt

TW-WebServer 1.0 - Denial of Service (1)
| multiple/dos/2[01;31m[K25[m[K02.pl

TW-WebServer 1.0 - Denial of Service (2)
| multiple/dos/2[01;31m[K25[m[K03.c

Typespeed 0.4.1 - Local Format String
| linux/local/[01;31m[K25[m[K106.c

Typo3 CMW_Linklist 1.4.1 Extension - SQL Injection
| php/webapps/[01;31m[K25[m[K186.txt

TYPSoft FTP Server 1.11 - 'RETR' Denial of Service
| windows/dos/1[01;31m[K25[m[K1.pl

UApplication Ublog 1.0.x - Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K317.txt

UApplication Ublog Reload 1.0.5 - 'Trackback.asp' Cross-Site Scripting
| asp/webapps/[01;31m[K25[m[K845.txt

UBBCentral UBB.Threads 5.5.1/6.x - 'addfav.php?main' SQL Injection
| php/webapps/[01;31m[K25[m[K901.txt

UBBCentral UBB.Threads 5.5.1/6.x - 'calendar.php' Multiple SQL
Injections                                    |
php/webapps/[01;31m[K25[m[K898.txt

UBBCentral UBB.Threads 5.5.1/6.x - 'download.php?Number' SQL Injection
| php/webapps/[01;31m[K25[m[K897.txt

UBBCentral UBB.Threads 5.5.1/6.x - 'grabnext.php?posted' SQL Injection
| php/webapps/[01;31m[K25[m[K903.txt

UBBCentral UBB.Threads 5.5.1/6.x - 'modifypost.php?Number' SQL
Injection                                     |
php/webapps/[01;31m[K25[m[K899.txt

UBBCentral UBB.Threads 5.5.1/6.x - 'notifymod.php?Number' SQL Injection
| php/webapps/[01;31m[K25[m[K902.txt

UBBCentral UBB.Threads 5.5.1/6.x - 'viewmessage.php?message' SQL
Injection                                    |
php/webapps/[01;31m[K25[m[K900.txt

UBBCentral UBB.Threads 6.0 - 'editpost.php' SQL Injection
| php/webapps/[01;31m[K25[m[K212.txt

UBBCentral UBB.Threads 6.0 - 'Printthread.php' SQL Injection
| php/webapps/[01;31m[K25[m[K457.c
```

UBBCentral UBB.Threads 6.1.1 - 'UBBThreads.php' SQL Injection
| php/webapps/298[01;31m[K25[m[K.txt

UBBCentral UBB.Threads 6.2.3/6.5 - 'calendar.php?Cat' Cross-Site Scripting |
php/webapps/248[01;31m[K25[m[K.txt

Ublog Reload 1.0.5 - 'blog_comment.asp?y' SQL Injection
| asp/webapps/[01;31m[K25[m[K844.txt

Ublog Reload 1.0.5 - 'index.asp' Multiple SQL Injections
| asp/webapps/[01;31m[K25[m[K843.txt

UC Gateway Investment SiteEngine 5.0 - 'announcements.php' SQL Injection |
php/webapps/3[01;31m[K25[m[K24.txt

UC Gateway Investment SiteEngine 5.0 - 'api.php' Open Redirection
| php/webapps/3[01;31m[K25[m[K23.txt

Ultimate PHP Board 1.8/1.9 - 'viewforum.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K654.txt

Ultimate PHP Board 1.8/1.9 - 'viewforum.php' SQL Injection
| php/webapps/[01;31m[K25[m[K655.txt

Ultimate PHP Board 1.8/1.9 - Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/[01;31m[K25[m[K8[01;31m[K25[m[K.txt

Ultimate PHP Board 1.8/1.9 - Weak Password Encryption
| php/webapps/[01;31m[K25[m[K838.pl

Ultimate Viral Media Script 1.0 - 'id' SQL Injection
| php/webapps/41[01;31m[K25[m[K5.txt

UltimatePOS 2.5 - Remote Code Execution
| php/webapps/45[01;31m[K25[m[K3.txt

UMI CMS 2.9 - Cross-Site Request Forgery
| php/webapps/[01;31m[K25[m[K449.txt

UML_Utilities User-Mode Linux - uml_utilities 20030903 UML_Net Slip Network Interface Denial of Service |
linux/dos/[01;31m[K25[m[K017.txt

University of Washington - imap LSUB Buffer Overflow (Metasploit)
| linux/remote/100[01;31m[K25[m[K.rb

Unreal Tournament 2004 - Null Pointer Remote Denial of Service
| multiple/dos/321[01;31m[K25[m[K.txt

UPC Ireland Cisco EPC 24[01;31m[K25[m[K Router / Horizon Box - WPA-PSK Handshake Information |
hardware/webapps/30358.txt

Uploader 0.1.5 - Multiple Vulnerabilities
| php/webapps/1[01;31m[K25[m[K70.txt

Upworthy Clone Script 1.1.0 - 'id' SQL Injection
| php/webapps/41[01;31m[K25[m[K4.txt

User Login and Management - Multiple Vulnerabilities
| php/webapps/4[01;31m[K25[m[K84.txt

Usermin 2.100 - Username Enumeration
| multiple/webapps/52[01;31m[K25[m[K4.py

V-Webmail 1.6.4 - '/includes/pear/Net/Socket.php?CONFIG[pear_dir]' Remote File Inclusion |
php/webapps/320[01;31m[K25[m[K.txt

Valdersoft Shopping Cart 3.0 - Multiple Input Validation Vulnerabilities |
php/webapps/[01;31m[K25[m[K301.txt

Vanderbilt IP-Camera CCPW30[01;31m[K25[m[K-IR / CVMW30[01;31m[K25[m[K-IR - Credentials Disclosure |
cgi/webapps/40263.txt

Vanderbilt IP-Camera CCPW30[01;31m[K25[m[K-IR / CVMW30[01;31m[K25[m[K-IR - Local File Disclosure |
cgi/webapps/40281.txt

Vanilla Forums 2.0.18.8 - Multiple Vulnerabilities
| php/webapps/[01;31m[K25[m[K720.txt

Vantage Linguistics AnswerWorks 4 - API ActiveX Control Buffer Overflow
| windows/remote/48[01;31m[K25[m[K.html

VBox Satellite Express 2.3.17.3 - Arbitrary Write
| windows/dos/382[01;31m[K25[m[K.txt

vBulletin 3.0 - Private Message HTML Injection
| php/webapps/2[01;31m[K25[m[K99.html

vBulletin 5.2.2 - Server-Side Request Forgery
| php/webapps/402[01;31m[K25[m[K.py

VCalendar 1.1.5 - Cross-Site Request Forgery
| php/webapps/17[01;31m[K25[m[K1.html

Verilink NetEngine 6100-4 Broadband Router - TFTP Packet Remote Denial of Service |
hardware/dos/2[01;31m[K25[m[K96.txt

```
VertrigoServ 2.[01;31m[K25[m[K - 'extensions.php' Script Cross-Site
Scripting                                              |
php/webapps/36508.txt

VeryPDF PDFView - ActiveX Component Heap Buffer Overflow
| windows/dos/3[01;31m[K25[m[K87.txt

Veyon 4.4.1 - 'VeyonService' Unquoted Service Path
| windows/local/499[01;31m[K25[m[K.txt

Video Cam Server 1.0 - Administrative Interface Authentication Bypass
| windows/remote/[01;31m[K25[m[K573.txt

video cam server 1.0 - Directory Traversal
| windows/remote/[01;31m[K25[m[K571.txt

Video Cam Server 1.0 - Full Path Disclosure
| windows/remote/[01;31m[K25[m[K572.txt

VideoDB 3.0.3 - Multiple Vulnerabilities
| php/webapps/152[01;31m[K25[m[K.txt

VideoLAN VLC Media Player 0.8.6e - Subtitle Parsing Local Buffer
Overflow                                       |
windows/local/5[01;31m[K25[m[K0.cpp

VideoLAN VLC Media Player 0.8.6i - '.tta' File Parsing Heap Overflow
(PoC)                                          |
multiple/dos/6[01;31m[K25[m[K2.txt

VideoLAN VLC Media Player 0.9.4 - '.ty' Local Buffer Overflow (SEH)
| windows/local/68[01;31m[K25[m[K.pl

VideoLAN VLC Media Player 1.1.8 - ModPlug ReadS3M Stack Buffer Overflow
(Metasploit)                                   |
windows/remote/17[01;31m[K25[m[K2.rb

VideoLAN VLC Media Player 2.0.0 - Mms Stream Handling Buffer Overflow
(Metasploit)                                     |
windows/remote/188[01;31m[K25[m[K.rb

VideoLAN VLC Media Player 2.2.1 - 'DecodeAdpcmImaQT' Buffer Overflow
| windows/dos/410[01;31m[K25[m[K.txt

VidiScript (Avatar) - Arbitrary File Upload
| php/webapps/6[01;31m[K25[m[K9.txt

Vim - 'mch_expand_wildcards()' Heap Buffer Overflow
| linux/remote/322[01;31m[K25[m[K.txt

VirtualBox 5.1.22 - Windows Process DLL Signature Bypass Privilege
Escalation                                       |
windows/local/424[01;31m[K25[m[K.txt
```

VirtueMart 3.1.14 - Persistent Cross-Site Scripting
| php/webapps/446[01;31m[K25[m[K.txt

VirusChaser 8.0 - Stack Buffer Overflow
| windows/dos/3[01;31m[K25[m[K22.py

VisNetic ActiveDefense 1.3.1 - GET Multiple Denial of Service
Vulnerabilities |
multiple/dos/2[01;31m[K25[m[K35.txt

VistaBB 2.x - 'functions_mod_user.php' Remote File Inclusion
| php/webapps/2[01;31m[K25[m[K1.pl

Visual Link Sharing Websites Builder Script 2.1.0 - SQL Injection
| php/webapps/41[01;31m[K25[m[K6.txt

Vivotek IP Cameras - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K25[m[K139.txt

VocalTec VGW120/VGW480 Telephony Gateway Remote H.2[01;31m[K25[m[K -
Denial of Service |
hardware/dos/24143.c

Vortex Portal 2.0 - 'content.php?act' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K261.txt

Vortex Portal 2.0 - 'index.php?act' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K260.txt

VoteBox 2.0 - 'Votebox.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K226.txt

Vox TG790 ADSL Router - Cross-Site Request Forgery (Add Admin)
| hardware/webapps/45[01;31m[K25[m[K2.txt

vTiger CRM 4.2 - 'calpath' Multiple Remote File Inclusions
| php/webapps/[01;31m[K25[m[K08.txt

vTiger CRM 5.2.1 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities (2) |
php/webapps/36[01;31m[K25[m[K5.txt

VX Search Enterprise 9.9.12 - 'Import Command' Local Buffer Overflow
| windows/local/4[01;31m[K25[m[K39.py

w-Agora 4.2.0 - 'quicklist.php' Remote Code Execution
| php/webapps/1[01;31m[K25[m[K0.php

Waibrasil - Local/Remote File Inclusion
| php/webapps/1[01;31m[K25[m[K62.txt

War FTP Daemon 1.8 - Remote Denial of Service
| windows/dos/[01;31m[K25[m[K063.pl

War Times - Remote Game Server Denial of Service
| windows/dos/[01;31m[K25[m[K680.txt

Warrior Kings 1.3 And Warrior Kings: Battles 1.23 - Remote Format String |
multiple/remote/[01;31m[K25[m[K691.txt

Warrior Kings: Battles 1.23 - Remote Denial of Service
| multiple/dos/[01;31m[K25[m[K692.txt

WBB3 rGallery 1.2.3 - 'UserGallery' Blind SQL Injection
| php/webapps/8[01;31m[K25[m[K4.pl

Weathermap 0.97c - 'mapname' Local File Inclusion
| php/webapps/261[01;31m[K25[m[K.txt

Web Calendar 4.1 - Authentication Bypass
| php/webapps/7[01;31m[K25[m[K2.txt

Web Protector 2.0 - Trivial Encryption
| multiple/remote/2[01;31m[K25[m[K22.pl

Web Wiz Forum 6.34 - Information Disclosure
| asp/webapps/2[01;31m[K25[m[K07.txt

Web4Future eDating Professional 5.0 - 'gift.php?cid' SQL Injection
| php/webapps/267[01;31m[K25[m[K.txt

web@all 1.1 - 'url' Cross-Site Scripting
| php/webapps/35[01;31m[K25[m[K3.txt

WebCalendar 0.9.45 - SQL Injection
| php/webapps/[01;31m[K25[m[K113.txt

WebChat 0.78 - 'login.php?rid' SQL Injection
| php/webapps/41[01;31m[K25[m[K.txt

WebCrossing WebX 5.0 - Cross-Site Scripting
| cgi/webapps/[01;31m[K25[m[K592.txt

WebCT Discussion Board 4.1 - HTML Injection
| php/webapps/[01;31m[K25[m[K381.txt

webframe 0.76 - Multiple File Inclusions
| php/webapps/80[01;31m[K25[m[K.txt

WeBid 1.0.6 - Multiple Vulnerabilities
| php/webapps/[01;31m[K25[m[K249.txt

Webify Blog - Arbitrary File Deletion
| php/webapps/21[01;31m[K25[m[K0.txt

```
Webkit (Apple Safari 4.0.5) - Blink Tag Stack Exhaustion Denial of
Service                                  |
windows/dos/124[01;31m[K25[m[K.html

Webkit (Apple Safari < 4.1.2/5.0.2 / Google Chrome <
5.0.375.1[01;31m[K25[m[K) - Memory Corruption                        |
windows/dos/14967.txt

Weblogic 3.1.8/4.0.4/4.5.1 - Remote Command Execution
| windows/remote/201[01;31m[K25[m[K.txt

WEBMIS CMS - Arbitrary File Upload
| php/webapps/39[01;31m[K25[m[K5.html

weborf 0.12.2 - Directory Traversal
| linux/remote/149[01;31m[K25[m[K.txt

WeBProdZ CMS - SQL Injection
| php/webapps/1[01;31m[K25[m[K22.txt

webSPELL 4.01.01 - 'getsquad' SQL Injection
| php/webapps/[01;31m[K25[m[K68.txt

webSPELL 4.01.02 - 'showonly' Blind SQL Injection
| php/webapps/33[01;31m[K25[m[K.pl

WebWasher Classic 2.2/2.3 - HTTP CONNECT Unauthorized Access
| multiple/remote/[01;31m[K25[m[K066.txt

WebWasher CSM 4.4.1 Build 752 Conf Script - Cross-Site Scripting
| cgi/webapps/[01;31m[K25[m[K350.txt

Wecodex Store Paypal 1.0 - SQL Injection
| php/webapps/447[01;31m[K25[m[K.txt

WFTPD Pro Server 3.[01;31m[K25[m[K - Site ADMN Remote Denial of Service
| windows/dos/3126.c

WFTPD Server 3.30 - Multiple Vulnerabilities
| linux/remote/1[01;31m[K25[m[K87.c

WhitSoft SlimServe HTTPd 1.0/1.1 - Directory Traversal
| windows/remote/[01;31m[K25[m[K933.txt

WHMCS 4.x - 'invoicefunctions.php?id' SQL Injection
| php/webapps/[01;31m[K25[m[K442.txt

Whois.Cart 2.2.x - 'profile.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K875.txt

Wifi Album 1.47 iOS - Command Injection
| ios/webapps/[01;31m[K25[m[K414.txt
```

Wifi Photo Transfer 2.1/1.1 PRO - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K25[m[K413.txt

Wikepage Opus 10 < 2006.2a (lng) - Remote Command Execution
| php/webapps/2[01;31m[K25[m[K2.pl

Winace UnAce 1.x - ACE Archive Directory Traversal
| linux/remote/[01;31m[K25[m[K150.txt

Winamp - MAKI Buffer Overflow (Metasploit)
| windows/local/21[01;31m[K25[m[K6.rb

Winamp 5.572 (Windows XP SP3 DE) - 'whatsnew.txt' Local Buffer Overflow
| windows/local/11[01;31m[K25[m[K6.pl

Winamp 5.572 - 'whatsnew.txt' (SEH) (Metasploit)
| windows/local/12[01;31m[K25[m[K5.rb

Winamp 5.572 - 'whatsnew.txt' Local Stack Overflow
| windows/local/11[01;31m[K25[m[K5.pl

WinArchiver 3.2 - Local Buffer Overflow (SEH)
| windows/local/[01;31m[K25[m[K131.py

Windows File Explorer Windows 10 Pro x64 - TAR Extraction
| windows/remote/523[01;31m[K25[m[K.py

WinFTP Server 1.6 - Denial of Service
| windows/dos/6[01;31m[K25[m[K.pl

WinRAR 5.80 (x64) - Denial of Service
| windows_x86-64/dos/475[01;31m[K25[m[K.txt

WinRM - VBS Remote Code Execution (Metasploit)
| windows/remote/2[01;31m[K25[m[K26.rb

Wireless Disk PRO 2.3 iOS - Multiple Vulnerabilities
| ios/webapps/[01;31m[K25[m[K412.txt

Wireless Photo Access 1.0.10 iOS - Multiple Vulnerabilities
| ios/webapps/[01;31m[K25[m[K415.txt

Wireless Repeater BE126 - Local File Inclusion
| hardware/webapps/4[01;31m[K25[m[K47.py

Wireshark - console.lua pre-loading (Metasploit)
| windows/remote/181[01;31m[K25[m[K.rb

Wireshark - hiqnet_display_data Static Out-of-Bounds Read
| multiple/dos/393[01;31m[K25[m[K.txt

Wirtualna Polska WPKontakt 3.0.1 - Remote Script Execution
| cgi/webapps/[01;31m[K25[m[K051.txt

```
Woltlab 1.1/2.x - 'Info-DB Info_db.php' Multiple SQL Injections
| php/webapps/264[01;31m[K25[m[K.pl

WoltLab Burning Board 2.3.1 - 'PMS.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K528.txt

WoltLab Burning Board 2.3.1 - 'thread.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K503.txt

WoltLab Burning Book 1.1.2 - SQL Injection
| php/webapps/[01;31m[K25[m[K79.pl

Woodall Creative - SQL Injection
| php/webapps/1[01;31m[K25[m[K76.txt

WordPress Core 1.5 - 'post.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K682.txt

WordPress Core 2.8.1 - 'url' Cross-Site Scripting
| php/webapps/9[01;31m[K25[m[K0.sh

WordPress Core 2.9 - Denial of Service
| php/dos/108[01;31m[K25[m[K.sh

WordPress Plugin Ad Manager WD 1.0.11 - Arbitrary File Download
| php/webapps/46[01;31m[K25[m[K2.txt

WordPress Plugin Adminimize 1.7.21 - 'page' Cross-Site Scripting
| php/webapps/363[01;31m[K25[m[K.txt

WordPress Plugin Audio 0.5.1 - 'showfile' Cross-Site Scripting
| php/webapps/35[01;31m[K25[m[K8.txt

WordPress Plugin Blue Admin 21.06.01 - Cross-Site Request Forgery
(CSRF)                                    |
php/webapps/509[01;31m[K25[m[K.html

WordPress Plugin BookX 1.7 - 'bookx_export.php' Local File Inclusion
| php/webapps/39[01;31m[K25[m[K1.txt

WordPress Plugin Category Grid View Gallery - 'ID' Cross-Site Scripting
| php/webapps/386[01;31m[K25[m[K.txt

WordPress Plugin CopySafe PDF Protection - Arbitrary File Upload
| php/webapps/39[01;31m[K25[m[K4.html

WordPress Plugin Download Manager 2.5 - Cross-Site Request Forgery
| php/webapps/47[01;31m[K25[m[K1.txt

WordPress Plugin Duplicate Page 4.4.1 - Stored Cross-Site Scripting
(XSS)                                      |
php/webapps/50[01;31m[K25[m[K6.txt
```

WordPress Plugin DZS-VideoGallery - Cross-Site Scripting / Command Injection | php/webapps/39[01;31m[K25[m[K0.txt

WordPress Plugin ENL NewsLetter - '/wp-admin/admin.php' SQL Injection | php/webapps/39[01;31m[K25[m[K3.txt

WordPress Plugin Fitness Calculators 1.9.5 - Cross-Site Request Forgery (CSRF) | php/webapps/503[01;31m[K25[m[K.html

WordPress Plugin Gift Voucher 1.0.5 - (Authenticated) 'template_id' SQL Injection | php/webapps/45[01;31m[K25[m[K5.txt

WordPress Plugin History Collection 1.1.1 - Arbitrary File Download | php/webapps/37[01;31m[K25[m[K4.txt

WordPress Plugin Image Manager - Arbitrary File Upload | php/webapps/103[01;31m[K25[m[K.txt

Wordpress Plugin ImageMagick-Engine 1.7.4 - Remote Code Execution (RCE) (Authenticated) | php/webapps/510[01;31m[K25[m[K.txt

WordPress Plugin InfusionSoft - Arbitrary File Upload (Metasploit) | php/remote/349[01;31m[K25[m[K.rb

WordPress Plugin jQuery Mega Menu 1.0 - Local File Inclusion | php/webapps/16[01;31m[K25[m[K0.txt

WordPress Plugin MM Forms Community 1.2.3 - SQL Injection | php/webapps/177[01;31m[K25[m[K.txt

WordPress Plugin Ninja Forms 3.6.[01;31m[K25[m[K - Reflected XSS | php/webapps/51644.py

WordPress Plugin OPS Old Post Spinner 2.2.1 - Local File Inclusion | php/webapps/16[01;31m[K25[m[K1.txt

WordPress Plugin Paypal Currency Converter Basic For WooCommerce - File Read | php/webapps/37[01;31m[K25[m[K3.txt

WordPress Plugin Postie 1.9.40 - Persistent Cross-Site Scripting | php/webapps/479[01;31m[K25[m[K.txt

WordPress Plugin ProPlayer 4.7.9.1 - SQL Injection | php/webapps/[01;31m[K25[m[K605.txt

WordPress Plugin RobotCPA V5 - Local File Inclusion | php/webapps/37[01;31m[K25[m[K2.txt

WordPress Plugin Simple Fields 0.2 - 0.3.5 - Local/Remote File Inclusion / Remote Code Execution | php/webapps/444[01;31m[K25[m[K.txt

```
WordPress Plugin Spider Catalog 1.4.6 - Multiple Vulnerabilities
| php/webapps/[01;31m[K25[m[K724.txt

WordPress Plugin Spider Event Calendar 1.3.0 - Multiple Vulnerabilities
| php/webapps/[01;31m[K25[m[K723.txt

WordPress Plugin Tagregator 0.6 - Cross-Site Scripting
| php/webapps/452[01;31m[K25[m[K.txt

WordPress Plugin Tera Charts (tera-charts) - '/charts/treemap.php?fn'
Directory Traversal                  |
php/webapps/39[01;31m[K25[m[K6.txt

WordPress Plugin Tera Charts (tera-charts) -
'/charts/zoomabletreemap.php?fn' Directory Traversal          |
php/webapps/39[01;31m[K25[m[K7.txt

WordPress Plugin Total Upkeep 1.14.9 - Database and Files Backup
Download                                  |
multiple/webapps/49[01;31m[K25[m[K2.txt

WordPress Plugin Uploader 1.0 - 'num' Cross-Site Scripting
| php/webapps/35[01;31m[K25[m[K5.txt

WordPress Plugin User Role Editor 3.12 - Cross-Site Request Forgery
| php/webapps/[01;31m[K25[m[K721.txt

WordPress Plugin User Role Editor < 4.[01;31m[K25[m[K - Privilege
Escalation                                                |
php/webapps/44595.rb

WordPress Plugin Videox7 UGC 2.5.3.2 - 'listid' Cross-Site Scripting
| php/webapps/35[01;31m[K25[m[K7.txt

WordPress Plugin W3 Total Cache - PHP Code Execution (Metasploit)
| php/remote/[01;31m[K25[m[K137.rb

WordPress Plugin wordTube 1.43 - 'wpPATH' Remote File Inclusion
| php/webapps/38[01;31m[K25[m[K.txt

WordPress Plugin WP Rss Poster - '/wp-admin/admin.php' SQL Injection
| php/webapps/39[01;31m[K25[m[K2.txt

WordPress Plugin WP User Frontend 3.5.[01;31m[K25[m[K - SQLi
(Authenticated)                                             |
php/webapps/50772.py

WordPress Plugin wp-FileManager - Arbitrary File Download
| php/webapps/[01;31m[K25[m[K440.txt

WordPress Plugin WP-Polls 2.x - Incorrect Flood Filter
| php/webapps/10[01;31m[K25[m[K6.txt
```

```
WordPress Plugin WP-Table Reloaded - 'id' Cross-Site Scripting
| php/webapps/38[01;31m[K25[m[K1.txt

WordPress Theme Highlight Premium - Cross-Site Request Forgery /
Arbitrary File Upload                     |
php/webapps/295[01;31m[K25[m[K.txt

WorkBoard 1.2 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K014.txt

Working Resources 1.7.x/2.15 BadBlue - 'ext.dll' Command Execution
| windows/remote/2[01;31m[K25[m[K11.txt

Working Resources BadBlue 2.55 - MFCISAPICommand Remote Buffer Overflow
(1)                                  |
windows/remote/[01;31m[K25[m[K166.c

Working Resources BadBlue 2.55 - MFCISAPICommand Remote Buffer Overflow
(2)                                  |
windows/remote/[01;31m[K25[m[K167.c

WowBB 1.6 - 'View_User.php' SQL Injection
| php/webapps/[01;31m[K25[m[K641.txt

WPanel 4.3.1 - Remote Code Execution (RCE) (Authenticated)
| multiple/webapps/50[01;31m[K25[m[K5.txt

WPS Office - 'Wpsio.dll' Stack Buffer Overflow
| windows/dos/[01;31m[K25[m[K140.txt

WSN Forum 1.3.4 - 'prestart.php' Remote Code Execution
| php/webapps/[01;31m[K25[m[K83.php

WSN Links 2.20 - 'comments.php' SQL Injection
| php/webapps/65[01;31m[K25[m[K.txt

WWWeb Concepts Events System 1.0 - 'login.asp' SQL Injection
| asp/webapps/[01;31m[K25[m[K790.txt

Wyse Winterm 11[01;31m[K25[m[KSE 4.2/4.4 - Remote Denial of Service
| multiple/dos/26145.c

WYSIWYG HTML Editor PRO 1.0 - Arbitrary File Download
| php/webapps/4[01;31m[K25[m[K71.txt

X-BLC 0.2.0 - 'get_read.php?section' SQL Injection
| php/webapps/8[01;31m[K25[m[K8.pl

X11R6 3.3.3 - Symlink
| linux/local/19[01;31m[K25[m[K7.c

XAMPP - 'Phonebook.php' Multiple Remote HTML Injection Vulnerabilities
| multiple/remote/[01;31m[K25[m[K391.txt
```

XAMPP - Insecure Default Password Disclosure
| multiple/dos/[01;31m[K25[m[K393.txt

XAMPP 1.7.4 - Cross-Site Scripting
| windows/remote/36[01;31m[K25[m[K8.txt

XAMPP for Windows 1.6.3a - Local Privilege Escalation
| windows/local/43[01;31m[K25[m[K.php

Xcode OpenBase 9.1.5 (OSX) - Local Privilege Escalation
| osx/local/[01;31m[K25[m[K65.pl

Xcode OpenBase 9.1.5 (OSX) - Root File Create Privilege Escalation
| osx/local/[01;31m[K25[m[K80.pl

Xen 3.x - pygrub Local Authentication Bypass
| linux/local/33[01;31m[K25[m[K5.txt

Xeneo Web Server 2.2.10 - Undisclosed Buffer Overflow (PoC)
| linux/dos/2[01;31m[K25[m[K27.c

Xeneo Web Server 2.2.9 - Denial of Service
| windows/dos/2[01;31m[K25[m[K16.pl

Xfire 1.6.4 - Remote Denial of Service
| windows/dos/[01;31m[K25[m[K71.pl

XGB 2.0 - Authentication Bypass
| php/webapps/[01;31m[K25[m[K090.txt

Xinetd 2.1.x/2.3.x - Rejected Connection Memory Leakage Denial of Service |
linux/dos/2[01;31m[K25[m[K08.sh

xinkaa Web station 1.0.3 - Directory Traversal
| multiple/remote/[01;31m[K25[m[K133.txt

Xion 1.0.1[01;31m[K25[m[K - '.m3u' Local SEH-Based Unicode Venetian Exploit |
windows/local/44243.pl

Xion Audio Player 1.0.1[01;31m[K25[m[K - Denial of Service
| windows/dos/14517.pl

Xion Player 1.0.1[01;31m[K25[m[K - Local Stack Buffer Overflow
| windows/local/14633.py

Xivo 1.2 - Arbitrary File Download
| php/webapps/2[01;31m[K25[m[K48.txt

Xlight FTP Server 1.[01;31m[K25[m[K/1.41 - 'PASS' Remote Buffer Overflow |
windows/dos/23468.pl

```
Xlrstats 2.0.1 - SQL Injection
| php/webapps/15[01;31m[K25[m[K1.txt

XM Easy Professional FTP Server 5.8.0 - Denial of Service
| windows/dos/10[01;31m[K25[m[K7.py

Xmame 0.102 - '-pb/-lang/-rec' Local Buffer Overflow
| linux/local/14[01;31m[K25[m[K.c

XMB Forum 1.8 - 'member.php' SQL Injection
| php/webapps/2[01;31m[K25[m[K21.c

XNova 0.8 sp1 - 'xnova_root_path' Remote File Inclusion
| php/webapps/6[01;31m[K25[m[K4.txt

Xonic.ru News 1.0 - 'script.php' Remote Command Execution
| php/webapps/2[01;31m[K25[m[K01.txt

XOOPS 'badliege' Module - 'id' SQL Injection
| php/webapps/31[01;31m[K25[m[K1.txt

XOOPS 'seminars' Module - 'id' SQL Injection
| php/webapps/31[01;31m[K25[m[K0.txt

Xoops 1.3.x/2.0 MyTextSanitizer - HTML Injection
| php/webapps/2[01;31m[K25[m[K39.txt

XOOPS Module module 3.0 - Directory Traversal
| php/webapps/[01;31m[K25[m[K074.txt

XOOPS Module tadbook2 - SQL Injection
| php/webapps/77[01;31m[K25[m[K.txt

XOOPS Module Tiny Event 1.01 - 'id' SQL Injection
| php/webapps/36[01;31m[K25[m[K.pl

Xpient - Cash Drawer Operation
| hardware/remote/[01;31m[K25[m[K987.txt

XRms 1.99.2 - 'case_title' Cross-Site Scripting
| php/webapps/323[01;31m[K25[m[K.txt

XWork < 2.0.11.2 - 'ParameterInterceptor' Class OGNL Security Bypass
| multiple/remote/3[01;31m[K25[m[K64.txt

Xxasp 3.3.2 - SQL Injection
| asp/webapps/10[01;31m[K25[m[K4.txt

Xymon 4.3.[01;31m[K25[m[K - useradm Command Execution (Metasploit)
| multiple/remote/47114.rb

YaBB 2.0 - Remote UsersRecentPosts Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K199.txt
```

YaBBSM 3.0.0 - 'Offline.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K53.txt

Yahoo! Messenger 5.x/6.0 - Offline Mode Status Remote Buffer Overflow
| windows/remote/[01;31m[K25[m[K196.txt

Yahoo! Messenger 5.x/6.0 - URL Handler Remote Denial of Service
| windows/dos/[01;31m[K25[m[K658.txt

Yahoo! Voice Chat ActiveX Control 1.0.0.43 - Remote Buffer Overflow
| windows/remote/2[01;31m[K25[m[K93.html

Yahoo! Widget < 4.0.5 - 'GetComponentVersion()' Remote Overflow
| windows/remote/4[01;31m[K25[m[K0.html

YapBB 1.2 Beta2 - 'yapbb_session.php' Remote File Inclusion
| php/webapps/[01;31m[K25[m[K94.php

YaPiG 0.9x - 'upload.php' Directory Traversal
| php/webapps/[01;31m[K25[m[K794.txt

YaPiG 0.9x - 'view.php' Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K793.txt

YaPiG 0.9x - Local/Remote File Inclusion
| php/webapps/[01;31m[K25[m[K792.txt

Yappa-ng 1.x/2.x - Cross-Site Scripting
| php/webapps/[01;31m[K25[m[K533.txt

Yappa-ng 1.x/2.x - Remote File Inclusion
| php/webapps/[01;31m[K25[m[K532.txt

yawcam 0.2.5 - Directory Traversal
| windows/remote/[01;31m[K25[m[K487.txt

Yaws 1.5x - Source Code Disclosure
| windows/remote/[01;31m[K25[m[K841.txt

YeaLink IP Phone Firmware 9.70.0.100 - Phone Call
| hardware/webapps/[01;31m[K25[m[K811.py

YepYep MTFTPD 0.2/0.3 - Remote CWD Argument Format String
| linux/remote/[01;31m[K25[m[K321.c

Yosemite Backup 8.70 - 'DtbClsLogin()' Remote Buffer Overflow
| windows/remote/3[01;31m[K25[m[K78.py

Youbin 2.5/3.0/3.4 - 'HOME' Buffer Overflow
| freebsd/local/2[01;31m[K25[m[K66.pl

Youngzsoft CMailServer 4.0 - 'RCPT TO' Buffer Overflow
| windows/dos/2[01;31m[K25[m[K82.pl

```
Youngzsoft CMailServer 4.0 - MAIL FROM Buffer Overflow
| windows/dos/2[01;31m[K25[m[K81.pl

YourFreeWorld Downline Builder Pro - 'tr.php' SQL Injection
| php/webapps/3[01;31m[K25[m[K63.txt

Yrch 1.0 - 'plug.inc.phppath' Remote File Inclusion
| php/webapps/30[01;31m[K25[m[K.pl

Zavio IP Cameras Firmware 1.6.03 - Multiple Vulnerabilities
| hardware/webapps/[01;31m[K25[m[K815.txt

Zeeways Shaadi Clone 2.0 - Authentication Bypass (2)
| php/webapps/3[01;31m[K25[m[K75.txt

Zen Cart 2008 - 'index.php?keyword' SQL Injection
| php/webapps/317[01;31m[K25[m[K.txt

Zen Help Desk 2.1 - Authentication Bypass
| php/webapps/88[01;31m[K25[m[K.txt

Zend Framework 1.9.6 - Multiple Input Validation Vulnerabilities /
Security Bypass                          |
php/remote/335[01;31m[K25[m[K.txt

ZenPhoto 1.4.3.3 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K25[m[K24.txt

ZeroBoard 4.1 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/[01;31m[K25[m[K1[01;31m[K25[m[K.txt

Zervit Web Server 0.4 - Directory Traversals
| windows/remote/1[01;31m[K25[m[K82.txt

Zervit Web Server 0.4 - Source Disclosure/Download
| windows/remote/1[01;31m[K25[m[K81.txt

Zhone GPON [01;31m[K25[m[K20 R4.0.2.566b - Crash (PoC)
| hardware/dos/35859.py

Ziepod+ 1.0 - CrossApplication Scripting
| windows/remote/1[01;31m[K25[m[K12.py

Ziggurat Farsi CMS - 'id' Cross-Site Scripting
| asp/webapps/338[01;31m[K25[m[K.txt

ZipGenius 6.3.1.[01;31m[K25[m[K52 - 'zgtips.dll' Local Stack Buffer
Overflow                                                |
windows/local/12326.py

ZKTeco ZKBioSecurity 3.0 - Cross-Site Request Forgery (Add Superadmin)
| jsp/webapps/403[01;31m[K25[m[K.html
```

ZOC Terminal 7.[01;31m[K25[m[K.5 - 'Script' Denial of Service (PoC)
| windows/dos/48302.py

ZOC Terminal v7.[01;31m[K25[m[K.5 - 'Private key file' Denial of
Service (PoC) |
windows/dos/48292.txt

Zoho ManageEngine Netflow Analyzer Professional 7.0.0.2 - Path
Traversal / Cross-Site Scripting |
jsp/webapps/464[01;31m[K25[m[K.html

Zomplog 3.9 - Cross-site scripting (XSS)
| php/webapps/516[01;31m[K25[m[K.txt

ZonPHP 2.[01;31m[K25[m[K - Remote Code Execution
| php/webapps/29091.txt

Zoo 2.10 - Parse.c Local Buffer Overflow
| linux/dos/274[01;31m[K25[m[K.txt

Zoom Media Gallery 2.1.2 - 'index.php' SQL Injection
| php/webapps/[01;31m[K25[m[K379.txt

Zope 2.11.2 - PythonScript Multiple Remote Denial of Service
Vulnerabilities |
multiple/dos/3[01;31m[K25[m[K81.txt

ZPanel - 'templateparser.class.php' Crafted Template Remote Command
Execution |
php/webapps/[01;31m[K25[m[K519.txt

ZYXEL P-660HN-T1H_IPv6 - Remote Configuration Editor / Web Server
Denial of Service |
hardware/dos/368[01;31m[K25[m[K.php

Shellcode Title
| Path

BSD/x86 - Bind ([01;31m[K25[m[K[01;31m[K25[m[K/TCP) Shell Shellcode
(167 bytes) |
bsd_x86/14795.c

BSD/x86 - Break chroot Shellcode (45 bytes)
| bsd_x86/13[01;31m[K25[m[K0.c

```
BSD/x86 - execve(/bin/cat /etc/master.passwd) | mail root@localhost
Shellcode (92 bytes)                    | bsd_x86/13[01;31m[K25[m[K5.c

BSD/x86 - execve(/bin/sh) + Encoded Shellcode (49 bytes)
| bsd_x86/13[01;31m[K25[m[K1.c

BSD/x86 - execve(/bin/sh) + Encoded Shellcode (57 bytes)
| bsd_x86/13[01;31m[K25[m[K2.c

BSD/x86 - Reverse (192.168.2.33:6969/TCP) Shell Shellcode (129 bytes)
| bsd/13[01;31m[K25[m[K6.c

BSD/x86 - Reverse (toroottеam.host.sk:2222/TCP) Shell Shellcode (93
bytes)                                  | bsd_x86/13[01;31m[K25[m[K4.c

BSDi/x86 - execve(/bin/sh) Shellcode (45 bytes)
| bsdi_x86/13[01;31m[K25[m[K7.c

BSDi/x86 - execve(/bin/sh) Shellcode (46 bytes)
| bsdi_x86/13[01;31m[K25[m[K8.c

FreeBSD/x86 - Bind (41[01;31m[K25[m[K4/TCP) Shell (/bin/sh) Shellcode
(115 bytes)                                          | freebsd_x86/43506.c

FreeBSD/x86 - Reverse (127.0.0.1:1337/TCP) Shell (/bin/sh) Shellcode
(81 bytes) (Generator)                | generator/160[01;31m[K25[m[K.c

Linux x86/x64 - Bind (4444/TCP) Shell Shellcode ([01;31m[K25[m[K1
bytes)                                                  | linux/39337.c

Linux/ARM (Raspberry Pi) - chmod 0777 /etc/shadow Shellcode (41 bytes)
| arm/21[01;31m[K25[m[K4.asm

Linux/ARM (Raspberry Pi) - execve(_/bin/sh__ [0]_ [0 vars]) Shellcode
(30 bytes)                            | arm/21[01;31m[K25[m[K3.asm

Linux/ARM (Raspberry Pi) - Reverse (10.1.1.2:0x1337/TCP) Shell
(/bin/sh) Shellcode (72 bytes)              |
arm/21[01;31m[K25[m[K2.asm

Linux/ARM - Reverse (192.168.1.124:4321/TCP) Shell (/bin/sh) Shellcode
(64 bytes)                            | arm/46[01;31m[K25[m[K8.s

Linux/IA32 - execve(/bin/sh) + 0xff-Free Shellcode (45 bytes)
| linux_x86/134[01;31m[K25[m[K.c

Linux/x64 - execve(/bin/bash) Shellcode (33 bytes)
| linux_x86-64/396[01;31m[K25[m[K.c

Linux/x64 - execve(/bin/sh) Shellcode ([01;31m[K25[m[K bytes) (1)
| linux_x86-64/39624.c
```

Linux/x64 - Fork Bomb Shellcode (11 bytes)
| linux_x86-64/4[01;31m[K25[m[K23.c

Linux/x64 - Kill All Processes Shellcode (19 bytes)
| linux_x86-64/4[01;31m[K25[m[K22.c

Linux/x64 - mkdir(ajit) Shellcode ([01;31m[K25[m[K bytes)
| linux_x86-64/41089.c

Linux/x86 - Bind (1472/TCP) Shell (/bin/sh) + IPv6 Shellcode
(1[01;31m[K25[m[K0 bytes) |
linux_x86/39723.c

Linux/x86 - Bind (31337/TCP) Shell + Polymorphic Shellcode
(1[01;31m[K25[m[K bytes) |
linux_x86/43698.c

Linux/x86 - Bind (4444/TCP) Shell (/bin/sh) + Null-Free Shellcode (75
bytes) | linux_x86/42[01;31m[K25[m[K4.c

Linux/x86 - Bind (6778/TCP) Shell + Polymorphic + XOR Encoded Shellcode
(1[01;31m[K25[m[K bytes) | linux_x86/14234.c

Linux/x86 - Bind (8000/TCP) Shell + Add Root User Shellcode
(2[01;31m[K25[m[K+ bytes) |
linux_x86/13318.s

Linux/x86 - cat .bash_history + base64 Encode + cURL
(http://localhost:8080) Shellcode (1[01;31m[K25[m[K bytes) |
linux_x86/46704.txt

Linux/x86 - chmod 0777 /etc/passwd + sys_chmod syscall Shellcode (39
bytes) | linux_x86/137[01;31m[K25[m[K.c

Linux/x86 - chmod 666 /etc/shadow + exit(0) Shellcode (30 bytes)
| linux_x86/133[01;31m[K25[m[K.c

Linux/x86 - execve(/bin/sh) Shellcode (21 bytes) (1)
| linux_x86/37[01;31m[K25[m[K1.asm

Linux/x86 - execve(/bin/sh) Shellcode ([01;31m[K25[m[K bytes)
| linux_x86/13670.c

Linux/x86 - execve(/bin/sh) Shellcode ([01;31m[K25[m[K bytes)
| linux_x86/47513.c

Linux/x86 - execve(_/bin/sh__ [_/bin/sh__ NULL]) Shellcode
([01;31m[K25[m[K bytes) |
linux_x86/13375.c

Linux/x86 - exit(0) Shellcode (5 bytes)
| linux_x86/46[01;31m[K25[m[K6.c

Linux/x86 - Force Reboot Shellcode (36 bytes)
| linux_x86/437[01;31m[K25[m[K.c

Linux/x86 - Fork Bomb Shellcode (9 bytes)
| linux_x86/4[01;31m[K25[m[K94.c

Linux/x86 - OpenSSL Encrypt (aes[01;31m[K25[m[K6cbc) Files (test.txt)
Shellcode (185 bytes) | linux_x86/46791.c

Linux/x86 - Read /etc/passwd Shellcode (58 Bytes) (2)
| linux_x86/46[01;31m[K25[m[K7.c

Linux/x86 - read(0_buf_[01;31m[K25[m[K41) + chmod(buf_4755) Shellcode
(23 bytes) | linux_x86/13406.c

Linux/x86 - Reverse
(127.[01;31m[K25[m[K5.[01;31m[K25[m[K5.[01;31m[K25[m[K4:9090/TCP) Shell
(/bin/zsh) Shellcode (80 bytes) |
linux_x86/40223.c

Linux/x86 - Reverse (192.168.1.10:31337/TCP) Shell Shellcode (92 bytes)
| linux_x86/[01;31m[K25[m[K497.c

Linux/x86 - Reverse (dynamic IP and port/TCP) Shell (/bin/sh) Shellcode
(86 bytes) | linux_x86/501[01;31m[K25[m[K.c

Linux/x86 - setuid(0) + execve(/bin/sh_0) Shellcode ([01;31m[K25[m[K
bytes) | linux_x86/43651.c

Linux/x86 - setuid(0) + setgid(0) + execve(/bin/sh_[/bin/sh_NULL]))
Shellcode ([01;31m[K25[m[K bytes) | linux_x86/43652.c

Linux/x86_64 - bash Shellcode with xor encoding
| linux_x86-64/51[01;31m[K25[m[K8.txt

Linux/x86_64 - Reverse (0.0.0.0:4444/TCP) Shell (/bin/sh) Shellcode
| linux_x86-64/470[01;31m[K25[m[K.c

Solaris/x86 - execve(/bin/sh) Shellcode (43 bytes)
| solaris_x86/436[01;31m[K25[m[K.c

Windows (9x/NT/2000/XP) - PEB Method Shellcode (29 bytes)
| windows_x86/135[01;31m[K25[m[K.c

Windows/x64 - Bind (2493/TCP) Shell + Password (h271508F) Shellcode
(8[01;31m[K25[m[K bytes) | windows_x86-
64/40981.c

Windows/x64 - WinExec Add-Admin (ROOT/I@mR00T$) Dynamic Null-Free
Shellcode (210 Bytes) | windows_x86-
64/48[01;31m[K25[m[K2.txt

Windows/x86 - CreateProcessA cmd.exe Shellcode ([01;31m[K25[m[K3 bytes)
| windows_x86/40246.c

Windows/x86 - InitiateSystemShutdownA() Shellcode (599 bytes)
| windows_x86/40[01;31m[K25[m[K9.c

Windows/x86 - ShellExecuteA(NULL_NULL__cmd.exe__NULL_NULL_1) Shellcode
([01;31m[K25[m[K0 bytes) | windows_x86/40005.c

Port: 3306

Exploit Title
| Path

Apple Safari 4 - 'reload()' Denial of Service
| windows/dos/[01;31m[K3306[m[K2.txt

Avax Vector 1.3 - 'avPreview.ocx' ActiveX Control Buffer Overflow
| windows/remote/[01;31m[K3306[m[K6.html

ClanSphere 2009 - 'text' Cross-Site Scripting
| php/webapps/[01;31m[K3306[m[K8.txt

Google Chrome 0.3.154 - 'JavaScript:' URI in 'Refresh' Header Cross-
Site Scripting |
multiple/remote/[01;31m[K3306[m[K4.txt

Horde 3.1 - 'Passwd' Module Cross-Site Scripting
| php/webapps/[01;31m[K3306[m[K5.txt

Joomla! 1.5.x - Cross-Site Scripting / Information Disclosure
| php/webapps/[01;31m[K3306[m[K1.php

MailEnable Professional/Enterprise 2.35 - Out of Bounds Denial of
Service |
windows/dos/[01;31m[K3306[m[K.pl

Microsoft Internet Explorer 6 - 'JavaScript:' URI in 'Refresh' Header
Cross-Site Scripting |
windows/remote/[01;31m[K3306[m[K3.txt

MLM Forex Market Plan Script 2.0.4 - 'newid' / 'eventid' SQL Injection
| php/webapps/4[01;31m[K3306[m[K.txt

MPlayer (r[01;31m[K3306[m[K4 Lite) - Local Buffer Overflow (ROP)
| windows/local/17124.pl

MPlayer Lite r[01;31m[K3306[m[K4 - '.m3u' Local Buffer Overflow (DEP Bypass) |
windows/local/17565.pl

MPlayer Lite r[01;31m[K3306[m[K4 - '.m3u' Local Overflow (SEH)
| windows/local/17013.pl

phpMyAdmin 3.3.0 - 'db' Cross-Site Scripting
| php/webapps/[01;31m[K3306[m[K0.txt

Snort 2.8.5 - Multiple Denial of Service Vulnerabilities
| linux/dos/3[01;31m[K3306[m[K.txt

thttpd 2.2x - 'defang' Remote Buffer Overflow
| linux/remote/2[01;31m[K3306[m[K.c

Winds3D Viewer 3 - 'GetURL()' Arbitrary File Download
| multiple/remote/[01;31m[K3306[m[K7.txt

Wireshark 1.8.12/1.10.5 - wiretap/mpeg.c Stack Buffer Overflow (Metasploit) |
windows/local/[01;31m[K3306[m[K9.rb

Shellcode Title
| Path

Linux/SPARC - Bind (8975/TCP) Shell + Null-Free Shellcode (284 bytes)
| linux_sparc/1[01;31m[K3306[m[K.c

Port: 443

Exploit Title
| Path

Aardvark Topsites 4.1 PHP - Multiple Vulnerabilities
| php/webapps/23[01;31m[K443[m[K.txt

Acrolinx Server < 5.2.5 - Directory Traversal
| windows/remote/[01;31m[K443[m[K45.txt

ActivDesk 3.0 - Multiple Vulnerabilities
| cgi/webapps/17[01;31m[K443[m[K.txt

Adobe JRun 4 - 'logfile' (Authenticated) Directory Traversal
| windows/remote/9[01;31m[K443[m[K.txt

Advantech WebAccess < 8.1 - webvrpcs DrawSrv.dll Path BwBuildPath Stack-Based Buffer Overflow |
windows/remote/[01;31m[K443[m[K76.py

AJ HYIP MERIDIAN - 'news.php?id' Blind SQL Injection
| php/webapps/1[01;31m[K443[m[K6.txt

AJ HYIP PRIME - 'welcome.php?id' Blind SQL Injection
| php/webapps/1[01;31m[K443[m[K5.txt

Allok AVI DivX MPEG to DVD Converter 2.6.1217 - Buffer Overflow (SEH)
| windows/local/[01;31m[K443[m[K63.py

Allok Quicktime to AVI MPEG DVD Converter 4.6.1217 - Stack-Based Buffer Overflow |
windows/local/[01;31m[K443[m[K30.py

Allok Video Joiner 4.6.1217 - Stack-Based Buffer Overflow
| windows/local/[01;31m[K443[m[K64.py

Allok WMV to AVI MPEG DVD WMV Converter 4.6.1217 - Buffer Overflow
| windows/local/[01;31m[K443[m[K65.py

Android Bluetooth - BNEP bnep_data_ind() Remote Heap Disclosure
| android/dos/[01;31m[K443[m[K26.py

Android Bluetooth - BNEP BNEP_SETUP_CONNECTION_REQUEST_MSG Out-of-Bounds Read |
android/dos/[01;31m[K443[m[K27.py

Apple macOS HelpViewer 10.12.1 - XSS Leads to Arbitrary File Execution / Arbitrary File Read |
macos/remote/41[01;31m[K443[m[K.html

Apple Quick Time Player (Windows) 7.7.3 - Out of Bound Read
| windows/dos/2[01;31m[K443[m[K7.py

```
Beanwebb Guestbook 1.0 - Unauthorized Administrative Access
| php/webapps/22[01;31m[K443[m[K.txt

Buddypress Xprofile Custom Fields Type 2.6.3 - Remote Code Execution
| php/webapps/4[01;31m[K443[m[K2.txt

Buffalo TeraStation TS-Series - Multiple Vulnerabilities
| hardware/webapps/24[01;31m[K443[m[K.txt

CAcert - 'analyse.php' Cross-Site Scripting
| php/webapps/32[01;31m[K443[m[K.txt

Calendarix 0.8.20071118 - SQL Injection
| php/webapps/11[01;31m[K443[m[K.txt

ChurchRota 2.6.4 - RCE (Authenticated)
| multiple/webapps/49[01;31m[K443[m[K.py

Cisco node-jos < 0.11.0 - Re-sign Tokens
| multiple/webapps/[01;31m[K443[m[K24.py

ClanSphere 2007.4 - 'cat_id' SQL Injection
| php/webapps/4[01;31m[K443[m[K.txt

ClipBucket - 'beats_uploader' Arbitrary File Upload (Metasploit)
| php/webapps/[01;31m[K443[m[K46.rb

Coship RT3052 Wireless Router - Persistent Cross-Site Scripting
| hardware/webapps/[01;31m[K443[m[K20.txt

Crashmail 1.6 - Stack-Based Buffer Overflow (ROP)
| linux/local/[01;31m[K443[m[K31.py

CS-Cart 1.3.2 - 'index.php' Cross-Site Scripting
| php/webapps/31[01;31m[K443[m[K.txt

D-Link DIR-850L Wireless AC1200 Dual Band Gigabit Cloud Router -
Authentication Bypass                     |
php/webapps/[01;31m[K443[m[K78.txt

DataLife Engine 9.7 - 'preview.php' PHP Code Injection
| php/webapps/2[01;31m[K443[m[K8.txt

Dell EMC NetWorker - Denial of Service
| linux/dos/[01;31m[K443[m[K32.py

Delta Industrial Automation DCISoft 1.12.09 - Local Stack Buffer
Overflow                                  |
windows/local/39[01;31m[K443[m[K.py

Digiappz Freekot 1.01 - ASP SQL Injection
| asp/webapps/28[01;31m[K443[m[K.html
```

```
DLink DIR-601 - Admin Password Disclosure
| hardware/webapps/[01;31m[K443[m[K88.txt

Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)
| php/webapps/[01;31m[K443[m[K55.php

DVD X Player Standard 5.5.3.9 - Buffer Overflow
| windows_x86/local/4[01;31m[K443[m[K8.txt

Easy Avi Divx Xvid to DVD Burner 2.9.11 - '.avi' Denial of Service
| windows/dos/[01;31m[K443[m[K38.py

Easy CD DVD Copy 1.3.24 - Local Buffer Overflow (SEH)
| windows/local/[01;31m[K443[m[K37.py

Eureka Email Client 2.2q - ERR Remote Buffer Overflow (Metasploit) (2)
| windows/remote/16[01;31m[K443[m[K.rb

Exodus Wallet (ElectronJS Framework) - Remote Code Execution
(Metasploit)                                    |
windows/remote/[01;31m[K443[m[K57.rb

Extcalendar 1.0 - Cross-Site Scripting
| php/webapps/27[01;31m[K443[m[K.txt

Faleemi Windows Desktop Software - (DDNS/IP) Local Buffer Overflow
| windows/local/[01;31m[K443[m[K82.py

Fast AVI MPEG Splitter 1.2 - Stack-Based Buffer Overflow
| windows/local/[01;31m[K443[m[K41.py

FlexPHPNews 0.0.6 / PRO - Authentication Bypass
| php/webapps/7[01;31m[K443[m[K.txt

Flip 3.0 - Remote Admin Creation
| php/webapps/[01;31m[K443[m[K5.pl

Flip 3.0 - Remote Password Hash Disclosure
| php/webapps/[01;31m[K443[m[K6.pl

Fortinet FortiMail 400 IBE - Multiple Vulnerabilities
| hardware/webapps/2[01;31m[K443[m[K5.txt

Free PHP photo Gallery script - Remote Command Execution
| php/webapps/1[01;31m[K443[m[K7.txt

Free PHP Photo Gallery Script - Remote File Inclusion
| php/webapps/1[01;31m[K443[m[K8.txt

FreePBX 2.5.2 - Zap Channel Addition Description Parameter Cross-Site
Scripting                              |
php/webapps/33[01;31m[K443[m[K.txt
```

```
Frog CMS 0.9.5 - Cross-Site Request Forgery (Add User)
| php/webapps/[01;31m[K443[m[K83.html

GitStack - Unsanitized Argument Remote Code Execution (Metasploit)
| windows/remote/[01;31m[K443[m[K56.rb

Google Chrome V8 - 'ElementsAccessorBase::CollectValuesOrEntriesImpl'
Type Confusion                        |
multiple/dos/[01;31m[K443[m[K94.js

Google Chrome V8 - 'Genesis::InitializeGlobal' Out-of-Bounds Read/Write
| multiple/dos/[01;31m[K443[m[K95.js

Google Software Updater macOS - Unsafe use of Distributed Objects
Privilege Escalation                    |
macos/local/[01;31m[K443[m[K07.m

Hikvision IP Camera versions 5.2.0 - 5.3.9 (Builds 140721 < 170109) -
Access Control Bypass                 |
xml/webapps/[01;31m[K443[m[K28.py

Homematic CCU2 2.29.23 - Arbitrary File Write
| cgi/webapps/[01;31m[K443[m[K61.rb

Homematic CCU2 2.29.23 - Remote Command Execution
| cgi/webapps/[01;31m[K443[m[K68.rb

Huawei Mate 7 - '/dev/hifi_misc' Privilege Escalation
| hardware/local/[01;31m[K443[m[K06.c

Intelbras Telefone IP TIP200 LITE - Local File Disclosure
| hardware/webapps/[01;31m[K443[m[K17.py

Internet Explorer - 'RegExp.lastMatch' Memory Disclosure
| windows/dos/[01;31m[K443[m[K12.js

IPSwitch IMail Server 8.0x - Remote Heap Overflow
| windows/remote/[01;31m[K443[m[K8.cpp

iScripts Easycreate 3.2.1 - Stored Cross-Site Scripting
| php/webapps/4[01;31m[K443[m[K6.txt

iScripts SonicBB 1.0 - Reflected Cross-Site Scripting (PoC)
| php/webapps/4[01;31m[K443[m[K4.txt

Job2C 4.2 - 'adtype' Local File Inclusion
| php/webapps/8[01;31m[K443[m[K.txt

Joomla! Component Acymailing Starter 5.9.5 - CSV Macro Injection
| php/webapps/[01;31m[K443[m[K69.txt

Joomla! Component AcySMS 3.5.0 - CSV Macro Injection
| php/webapps/[01;31m[K443[m[K70.txt
```

Joomla! Component com_forme 1.0.5 - Multiple Vulnerabilities
| php/webapps/15[01;31m[K443[m[K.txt

Joomla! Component com_jomtube - 'user_id' Blind SQL Injection
| php/webapps/1[01;31m[K443[m[K4.txt

Joomla! Component com_szallasok - 'id' SQL Injection
| php/webapps/37[01;31m[K443[m[K.txt

Joomla! Component Fields - SQLi Remote Code Execution (Metasploit)
| php/webapps/[01;31m[K443[m[K58.rb

Kamailio 5.1.1 / 5.1.0 / 5.0.0 - Off-by-One Heap Overflow
| linux/dos/[01;31m[K443[m[K16.py

Kohana Framework 2.3.3 - Directory Traversal
| php/webapps/2[01;31m[K443[m[K6.txt

KYOCERA Multi-Set Template Editor 3.4 - Out-Of-Band XML External Entity
Injection | xml/webapps/4[01;31m[K443[m[K0.txt

KYOCERA Net Admin 3.4 - Cross-Site Request Forgery (Add Admin)
| linux/webapps/4[01;31m[K443[m[K1.txt

LabF nfsAxe 3.7 - Privilege Escalation
| windows/local/[01;31m[K443[m[K42.txt

Laravel Log Viewer < 0.13.0 - Local File Download
| php/webapps/[01;31m[K443[m[K43.py

Liferay 6.1.0 CE - Privilege Escalation
| php/webapps/38[01;31m[K443[m[K.txt

LifeSize ClearSea 3.1.4 - Directory Traversal
| windows/webapps/[01;31m[K443[m[K90.py

Lighttpd 1.4.17 - FastCGI Header Overflow Arbitrary Code Execution
| linux/remote/[01;31m[K443[m[K7.c

LILDBI - Arbitrary File Upload
| php/webapps/14[01;31m[K443[m[K.txt

Linux Kernel - 'mincore()' Heap Page Disclosure (PoC)
| linux/dos/[01;31m[K443[m[K04.c

Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (2)
| linux/dos/[01;31m[K443[m[K05.c

Linux Kernel 4.13 (Debian 9) - Local Privilege Escalation
| linux/local/[01;31m[K443[m[K03.c

```
Linux Kernel < 3.16.39 (Debian 8 x64) - 'inotfiy' Local Privilege
Escalation                                | linux_x86-
64/local/[01;31m[K443[m[K02.c

Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak
| linux/local/[01;31m[K443[m[K25.c

Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset'
Local Privilege Escalation          | linux_x86-
64/local/[01;31m[K443[m[K00.c

Linux Kernel < 4.5.1 - Off-By-One (PoC)
| linux/dos/[01;31m[K443[m[K01.c

Maxthon Browser 2.1.4.[01;31m[K443[m[K - Unicode Remote Denial of
Service (PoC)                                          |
windows/dos/6434.html

MegaBrowser < 0.71b - Multiple Vulnerabilities
| multiple/webapps/43[01;31m[K443[m[K.txt

Microsoft Edge Chakra JIT - Stack-to-Heap Copy (Incomplete Fix) (1)
| windows/dos/[01;31m[K443[m[K96.js

Microsoft Edge Chakra JIT - Stack-to-Heap Copy (Incomplete Fix) (2)
| windows/dos/[01;31m[K443[m[K97.js

Microsoft Internet Explorer 8/9 - Steal Any Cookie
| windows/webapps/2[01;31m[K443[m[K2.txt

Microsoft Visual Basic Enterprise 6.0 SP6 - Code Execution
| windows/local/[01;31m[K443[m[K1.py

Microsoft Windows - Desktop Bridge VFS Privilege Escalation
| windows_x86-64/local/[01;31m[K443[m[K13.txt

Microsoft Windows - Desktop Bridge Virtual Registry Arbitrary File
Read/Write Privilege Escalation         |
windows/local/[01;31m[K443[m[K14.ps1

Microsoft Windows - Desktop Bridge Virtual Registry NtLoadKey Arbitrary
File Read/Write Privilege Escalati |
windows/local/[01;31m[K443[m[K15.txt

Microsoft Windows Firewall Control - Unquoted Service Path Privilege
Escalation                              |
windows/local/40[01;31m[K443[m[K.txt

Microsoft Windows Kernel - 'nt!KiDispatchException' 64-bit Stack Memory
Disclosure                          | windows_x86-
64/dos/[01;31m[K443[m[K10.cpp
```

Microsoft Windows Kernel - 'nt!NtWaitForDebugEvent' 64-bit Stack Memory Disclosure | windows_x86-64/dos/[01;31m[K443[m[K11.cpp

Microsoft Windows Kernel - 'NtQueryInformationThread(ThreadBasicInformation)' 64-bit Stack Memory Disclosu | windows_x86-64/dos/[01;31m[K443[m[K09.cpp

Microsoft Windows Kernel - 'NtQueryVirtualMemory(MemoryMappedFilenameInformation)' 64-bit Pool Memory Disc | windows_x86-64/dos/[01;31m[K443[m[K08.cpp

Microsoft Windows Remote Assistance - XML External Entity Injection | windows/webapps/[01;31m[K443[m[K52.txt

MiniCMS 1.10 - Cross-Site Request Forgery | php/webapps/[01;31m[K443[m[K62.html

Modelbook - 'casting_view.php' SQL Injection | php/webapps/12[01;31m[K443[m[K.txt

Moxa AWK-3131A 1.4 < 1.7 - 'Username' OS Command Injection | hardware/remote/[01;31m[K443[m[K98.py

MyBB Plugin Last User's Threads in Profile Plugin 1.2 - Persistent Cross-Site Scripting | php/webapps/[01;31m[K443[m[K39.txt

MybbCentral TagCloud 2.0 - 'Topic' HTML Injection | php/webapps/3[01;31m[K443[m[K8.txt

Nagios XI - Multiple Cross-Site Request Forgery Vulnerabilities | linux/remote/3[01;31m[K443[m[K1.html

Netgear Genie 2.4.64 - Unquoted Service Path | windows/local/50[01;31m[K443[m[K.txt

Netscape Enterprise Server 3.51/3.6 - JHTML View Source | multiple/remote/19[01;31m[K443[m[K.txt

neuron news 1.0 - 'index.php?q' Local File Inclusion | php/webapps/[01;31m[K443[m[K9.txt

Newswriter SW 1.4.2 - 'main.inc.php' Remote File Inclusion | php/webapps/2[01;31m[K443[m[K.txt

OneCMS 2.4 - 'abc' SQL Injection | php/webapps/[01;31m[K443[m[K3.pl

Open-AuditIT Professional 2.1 - Cross-Site Request Forgery | multiple/webapps/[01;31m[K443[m[K60.txt

```
Open-AuditIT Professional 2.1 - Cross-Site Scripting
| php/webapps/[01;31m[K443[m[K54.txt

OpenCMS 10.5.3 - Cross-Site Request Forgery
| php/webapps/[01;31m[K443[m[K91.html

OpenCMS 10.5.3 - Cross-Site Scripting
| php/webapps/[01;31m[K443[m[K92.txt

OpenX - 'phpAdsNew' Remote File Inclusion
| php/webapps/1[01;31m[K443[m[K2.txt

Opera Web Browser < 11.60 - Denial of Service / Multiple
Vulnerabilities                                       |
windows/dos/36[01;31m[K443[m[K.txt

osCommerce 2.3.4.1 - Remote Code Execution
| php/webapps/[01;31m[K443[m[K74.py

PaoLink 1.0 - 'scrivi.php' Cross-Site Scripting
| php/webapps/34[01;31m[K443[m[K.txt

pfSense UTM Platform 2.0.1 - Cross-Site Scripting
| freebsd/webapps/2[01;31m[K443[m[K9.txt

PHP 4.x/5.0.x - Arbitrary File Upload GLOBAL Variable Overwrite
| php/remote/26[01;31m[K443[m[K.php

PHP weby directory software 1.2 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K443[m[K3.txt

phpBazar Admin - Information Disclosure
| php/webapps/1[01;31m[K443[m[K9.txt

phpBB Plus 1.53 - 'phpbb_root_path' Remote File Inclusion
| php/webapps/[01;31m[K443[m[K4.txt

Pi-hole < 4.4 - Authenticated Remote Code Execution / Privileges
Escalation                                    |
linux/webapps/48[01;31m[K443[m[K.py

Piwigo Plugin User Tag 0.9.0 - Cross-Site Scripting
| php/webapps/42[01;31m[K443[m[K.txt

PMB Services 3.0.13 - Multiple Remote File Inclusions
| php/webapps/3[01;31m[K443[m[K.txt

Portable Document Format - Specification Signature Collision
| windows/remote/3[01;31m[K443[m[K7.txt

Preation Eden Platform 27.7.2010 - Multiple HTML Injection
Vulnerabilities                                     |
php/webapps/3[01;31m[K443[m[K0.txt
```

```
ProcessMaker - Plugin Upload (Metasploit)
| php/webapps/[01;31m[K443[m[K99.rb

QQPlayer - '.cue' File Buffer Overflow
| windows/local/1[01;31m[K443[m[K1.py

Quick Search 1.1.0.189 - Buffer Overflow (SEH)
| windows/dos/25[01;31m[K443[m[K.txt

RapidLeech Scripts - Arbitrary File Upload
| php/webapps/1[01;31m[K443[m[K0.txt

Ruby on Rails - JSON Processor YAML Deserialization Code Execution
(Metasploit)                              |
multiple/remote/2[01;31m[K443[m[K4.rb

ScreenStream 3.0.15 - Denial of Service
| android/dos/46[01;31m[K443[m[K.py

Secutech RiS-11/RiS-22/RiS-33 - Remote DNS Change
| hardware/webapps/[01;31m[K443[m[K93.sh

ServletExec - Directory Traversal / Authentication Bypass
| multiple/remote/3[01;31m[K443[m[K9.txt

Simple Directory Listing 2.1 - 'SDL2.php' Cross-Site Scripting
| php/webapps/3[01;31m[K443[m[K3.txt

SmallBiz eShop - 'content_id' SQL Injection
| php/webapps/5[01;31m[K443[m[K.txt

Streamline PHP Media Server 1.0-beta4 - Remote File Inclusion
| php/webapps/[01;31m[K443[m[K0.txt

Sun jre1.6.0_X - isInstalled.dnsResolve Function Overflow
| multiple/dos/[01;31m[K443[m[K2.html

swDesk - Multiple Vulnerabilities
| php/webapps/18[01;31m[K443[m[K.txt

SysGauge 4.5.18 - Local Denial of Service
| windows/dos/[01;31m[K443[m[K72.py

Systematic SitAware - NVG Denial of Service
| xml/dos/[01;31m[K443[m[K75.py

Tenda FH303/A300 Firmware v5.07.68_EN - Remote DNS Change
| asp/webapps/[01;31m[K443[m[K81.txt

Tenda N11 Wireless Router 5.07.43_en_NEX01 - Remote DNS Change
| hardware/webapps/[01;31m[K443[m[K53.sh
```

Tenda W3002R/A302/w309r Wireless Router v5.07.64_en - Remote DNS Change (PoC) | asp/webapps/[01;31m[K443[m[K80.txt

Tenda W308R v2 Wireless Router 5.07.48 - (Cookie Session) Remote DNS Change | asp/webapps/[01;31m[K443[m[K73.txt

Tenda W316R Wireless Router 5.07.50 - Remote DNS Change | asp/webapps/[01;31m[K443[m[K77.txt

TinyWebGallery v2.5 - Remote Code Execution (RCE) | php/webapps/51[01;31m[K443[m[K.txt

TL-WR720N 150Mbps Wireless N Router - Cross-Site Request Forgery | hardware/webapps/[01;31m[K443[m[K35.js

Tunnelblick - Local Privilege Escalation (2) | osx/local/20[01;31m[K443[m[K.sh

TwonkyMedia Server 7.0.11-8.5 - Directory Traversal | multiple/webapps/[01;31m[K443[m[K50.py

TwonkyMedia Server 7.0.11-8.5 - Persistent Cross-Site Scripting | multiple/webapps/[01;31m[K443[m[K51.txt

TYPO3 Extension ke DomPDF - Remote Code Execution | php/webapps/35[01;31m[K443[m[K.txt

Vehicle Sales Management System - Multiple Vulnerabilities | php/webapps/[01;31m[K443[m[K18.txt

VideoFlow Digital Video Protection (DVP) 2.10 - Directory Traversal | perl/webapps/[01;31m[K443[m[K86.txt

VideoFlow Digital Video Protection (DVP) 2.10 - Hard-Coded Credentials | hardware/webapps/[01;31m[K443[m[K87.txt

VideoLAN VLC Media Player 0.8.6a - Denial of Service (2) | windows/dos/29[01;31m[K443[m[K.py

Vtiger CRM 6.3.0 - (Authenticated) Arbitrary File Upload (Metasploit) | php/webapps/[01;31m[K443[m[K79.rb

WampServer 3.1.1 - Cross-Site Scripting / Cross-Site Request Forgery | php/webapps/[01;31m[K443[m[K84.txt

WampServer 3.1.2 - Cross-Site Request Forgery | php/webapps/[01;31m[K443[m[K85.html

WebLog Expert Enterprise 9.4 - Privilege Escalation | windows/local/[01;31m[K443[m[K89.txt

```
WebPortal CMS 0.7.4 - 'download.php' SQL Injection
| php/webapps/6[01;31m[K443[m[K.pl

WebRTC - VP9 Processing Use-After-Free
| multiple/dos/45[01;31m[K443[m[K.txt

WM Recorder 16.8.1 - Denial of Service
| windows/dos/[01;31m[K443[m[K33.py

WooCommerce CSV-Importer-Plugin 3.3.6 - Remote Code Execution
| php/webapps/4[01;31m[K443[m[K3.txt

WordPress Plugin Activity Log 2.4.0 - Stored Cross-Site Scripting
| php/webapps/4[01;31m[K443[m[K7.txt

WordPress Plugin ARforms 3.7.1 - Arbitrary File Deletion
| php/webapps/47[01;31m[K443[m[K.rb

WordPress Plugin Contact Form 7 to Database Extension 2.10.32 - CSV
Injection                                |
php/webapps/[01;31m[K443[m[K67.txt

WordPress Plugin File Upload 4.3.2 - Stored Cross-Site Scripting
| php/webapps/44[01;31m[K443[m[K.txt

WordPress Plugin Google Drive 2.2 - Remote Code Execution
| php/webapps/4[01;31m[K443[m[K5.txt

WordPress Plugin Relevanssi 4.0.4 - Reflected Cross-Site Scripting
| php/webapps/[01;31m[K443[m[K66.txt

WordPress Plugin ShortCode 0.2.3 - Local File Inclusion
| php/webapps/3[01;31m[K443[m[K6.txt

WordPress Plugin Site Editor 1.1.1 - Local File Inclusion
| php/webapps/[01;31m[K443[m[K40.txt

WordPress Plugin WP Security Audit Log 3.1.1 - Sensitive Information
Disclosure                               |
php/webapps/[01;31m[K443[m[K71.txt

WordPress Theme Persuasion 2.x - Arbitrary File Download / File
Deletion                                 |
php/webapps/30[01;31m[K443[m[K.txt

Wowd - 'index.html' Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K443[m[K2.txt

WU-IMAPd 2000/2001 - Partial Mailbox Attribute Remote Buffer Overflow
(2)                                      |
linux/remote/21[01;31m[K443[m[K.c
```

WUZHI CMS 4.1.0 - Cross-Site Request Forgery (Add Admin)
| php/webapps/4[01;31m[K443[m[K9.txt

XenForo 2 - CSS Loader Denial of Service
| php/dos/[01;31m[K443[m[K36.py

ZipCentral - '.zip' Local Buffer Overflow (SEH)
| windows/local/1[01;31m[K443[m[K3.pl

Shellcode Title
| Path

Linux/CRISv32 Axis Communication - Reverse
(192.168.57.1:[01;31m[K443[m[K/TCP) Shell (/bin/sh) Shellcode (189
bytes) | linux_crisv32/40128.c

Linux/x64 - Reverse (192.168.55.42:[01;31m[K443[m[K/TCP) Shell + Stager
+ Null-Free Shellcode (188 bytes) | linux_x86-
64/47784.txt

Linux/x86 - Bind (9[01;31m[K443[m[K/TCP) Shell + fork() + Null-Free
Shellcode (113 bytes) | linux_x86/44602.c

Linux/x86 - chmod(/etc/shadow_ 0666) + ASCII Shellcode
([01;31m[K443[m[K bytes) |
linux_x86/43696.c

Linux/x86 - Egghunter + Null-Free Shellcode (11 Bytes)
| linux_x86/[01;31m[K443[m[K34.c

Linux/x86 - execve(/bin/sh) Shellcode (18 bytes)
| linux_x86/[01;31m[K443[m[K21.c

Linux/x86 - execve(/bin/sh) Shellcode (29 bytes)
| linux_x86/13[01;31m[K443[m[K.c

Solaris/MIPS - Reverse (10.0.0.3:4[01;31m[K443[m[K4/TCP) Shell + XNOR
Encoded Traffic Shellcode (600 bytes) (Generator) | generator/13491.c

---

Port: 445

```
---------------------------------------------------------------------------------------- ----------
----------
Exploit Title
|  Path

---------------------------------------------------------------------------------------- ----------
----------
2Point Solutions - 'cmspages.php' SQL Injection
| php/webapps/17[01;31m[K445[m[K.txt

ActiveKB KnowledgeBase 2.x - 'catId' SQL Injection
| php/webapps/[01;31m[K445[m[K9.txt

ActualAnalyzer Lite 2.81 - Command Execution
| php/webapps/3[01;31m[K445[m[K0.py

AdaptCMS 2.0.4 - 'config.php?question' SQL Injection
| php/webapps/2[01;31m[K445[m[K2.txt

Adobe Flash - Info Leak in Image Inflation
| multiple/dos/[01;31m[K445[m[K28.txt

Adobe Flash - Out-of-Bounds Write in blur Filtering
| multiple/dos/[01;31m[K445[m[K29.txt

Adobe Flash - Overflow in Slab Rendering
| multiple/dos/[01;31m[K445[m[K27.txt

Adobe Flash - Overflow when Playing Sound
| multiple/dos/[01;31m[K445[m[K26.txt

Adobe Reader PDF - Client Side Request Injection
| windows/local/[01;31m[K445[m[K73.txt

AirDrop 2.0 - Denial of Service (DoS)
| android/dos/46[01;31m[K445[m[K.c

AirTies-[01;31m[K445[m[K0 - Unauthorized Remote Reboot (Denial of
Service)                                                 |
hardware/dos/18336.pl

Allok AVI to DVD SVCD VCD Converter 4.0.1217 - Buffer Overflow (SEH)
| windows/local/[01;31m[K445[m[K49.py

Allok Video to DVD Burner 2.6.1217 - Buffer Overflow (SEH)
| windows/local/[01;31m[K445[m[K18.py

Amiro.CMS 5.4 - Multiple Input Validation Vulnerabilities
| php/webapps/3[01;31m[K445[m[K9.txt

Android Bluetooth - 'Blueborne' Information Leak (1)
| android/remote/[01;31m[K445[m[K54.py
```

```
Android Bluetooth - 'Blueborne' Information Leak (2)
| android/remote/[01;31m[K445[m[K55.py

Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - Arbitrary Code Execution
| multiple/remote/[01;31m[K445[m[K56.py

Apache Struts2 2.0.0 < 2.3.15 - Prefixed Parameters OGNL Injection
| multiple/webapps/[01;31m[K445[m[K83.txt

Apple macOS 10.13.2 - Double mach_port_deallocate in kextd due to
Failure to Comply with MIG Ownership Rul |
macos/dos/[01;31m[K445[m[K61.txt

Apple macOS/iOS - ReportCrash mach port Replacement due to Failure to
Respect MIG Ownership Rules          |
multiple/dos/[01;31m[K445[m[K62.c

ArrowChat 1.5.61 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K445[m[K1.txt

Articles Directory - Authentication Bypass
| php/webapps/12[01;31m[K445[m[K.txt

Ask.com/AskJeeves Toolbar Toolbar 4.0.2.53 - ActiveX Remote Buffer
Overflow                                 |
windows/remote/[01;31m[K445[m[K2.html

ASUS infosvr - Authentication Bypass Command Execution (Metasploit)
| hardware/remote/[01;31m[K445[m[K24.rb

BaBB 2.8 - Remote Code Injection
| php/webapps/9[01;31m[K445[m[K.py

Barco ClickShare CSE-200 - Remote Denial of Service
| hardware/dos/4[01;31m[K445[m[K6.py

Blog Master Pro 1.0 - CSV Injection
| php/webapps/[01;31m[K445[m[K35.txt

Bopup Communications Server - Remote Buffer Overflow (Metasploit)
| windows/remote/16[01;31m[K445[m[K.rb

Build Smart ERP 21.0817 - 'eidValue' SQL Injection (Unauthenticated)
| asp/webapps/50[01;31m[K445[m[K.txt

Call of Duty Modern Warefare 2 - Buffer Overflow
| windows/remote/[01;31m[K445[m[K82.txt

Chrome V8 JIT - 'AwaitedPromise' Update Bug
| multiple/dos/[01;31m[K445[m[K40.js

Chrome V8 JIT - 'NodeProperties::InferReceiverMaps' Type Confusion
| multiple/dos/[01;31m[K445[m[K30.js
```

```
Chrome V8 JIT - Arrow Function Scope Fixing Bug
| multiple/dos/[01;31m[K445[m[K41.js

Cisco Smart Install - Crash (PoC)
| hardware/dos/4[01;31m[K445[m[K1.py

CMS Lokomedia - Multiple Cross-Site Scripting / HTML Injection
Vulnerabilities                                 |
php/webapps/37[01;31m[K445[m[K.txt

Cobub Razor 0.8.0 - SQL injection
| php/webapps/4[01;31m[K445[m[K4.txt

Cockpit CMS 0.4.4 < 0.5.5 - Server-Side Request Forgery
| php/webapps/[01;31m[K445[m[K67.txt

Comersus Backoffice 4.x/5.0/6.0 - '/comersus/database/comersus.mdb'
Direct Request Database Disclosure     |
asp/webapps/26[01;31m[K445[m[K.pl

Critical Path InJoin Directory Server 4.0 - File Disclosure
| multiple/remote/21[01;31m[K445[m[K.txt

CSP MySQL User Manager 2.3.1 - Authentication Bypass
| linux/webapps/[01;31m[K445[m[K89.txt

D-Link DIR-600 / DIR-300 (Rev B) - Multiple Vulnerabilities
| hardware/webapps/2[01;31m[K445[m[K3.txt

DeviceLock Plug and Play Auditor 5.72 - Unicode Buffer Overflow (SEH)
| windows/local/[01;31m[K445[m[K90.txt

DFD Cart 1.1 - Multiple Remote File Inclusions
| php/webapps/[01;31m[K445[m[K1.txt

Discussion Web 4 - Remote Database Disclosure
| asp/webapps/7[01;31m[K445[m[K.txt

DLINK DCS-5020L - Remote Code Execution (PoC)
| hardware/webapps/[01;31m[K445[m[K80.txt

DM FileManager 3.9.11 - Arbitrary File Upload
| php/webapps/1[01;31m[K445[m[K7.txt

Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code
(Metasploit)                                    |
php/webapps/[01;31m[K445[m[K57.rb

Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution
(PoC)                                  |
php/webapps/[01;31m[K445[m[K42.txt
```

```
Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure
| php/webapps/[01;31m[K445[m[K01.txt

DWebPro 8.4.2 - Multiple Vulnerabilities
| windows/remote/40[01;31m[K445[m[K.txt

Easy File Sharing Web Server 7.2 - 'UserID' Remote Buffer Overflow (DEP
Bypass)                              |
windows/remote/[01;31m[K445[m[K22.py

Easy MPEG to DVD Burner 1.7.11 - Local Buffer Overflow (SEH)
| windows/local/[01;31m[K445[m[K65.py

EasyFTP Server 1.7.0.11 - 'LIST' (Authenticated) Remote Buffer Overflow
(Metasploit)                         |
windows/remote/1[01;31m[K445[m[K1.rb

EasyMail MessagePrinter Object - 'emprint.dll 6.0.1.0' Remote Buffer
Overflow                                |
windows/remote/4[01;31m[K445[m[K.html

EB Design Pty Ltd - 'EBCRYPT.dll 2.0' Multiple Remote Vulnerabilities
| windows/remote/[01;31m[K445[m[K3.html

Elastic Path 4.1 - '/manager/getImportFileRedirect.jsp?file' Traversal
Arbitrary File Access               |
jsp/webapps/31[01;31m[K445[m[K.txt

Ericsson-LG iPECS NMS A.1Ac - Cleartext Credential Disclosure
| php/webapps/[01;31m[K445[m[K15.py

Eterm LibAST < 0.7 - '-X' Option Privilege Escalation
| linux/local/1[01;31m[K445[m[K.c

Exim < 4.90.1 - 'base64d' Remote Code Execution
| linux/remote/[01;31m[K445[m[K71.py

Femitter FTP Server 1.04 - Directory Traversal
| windows/remote/15[01;31m[K445[m[K.txt

Free Monthly Websites 2.0 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K445[m[K4.txt

FreeBSD 9.1 - 'ftpd' Remote Denial of Service
| freebsd/dos/2[01;31m[K445[m[K0.txt

Frog CMS 0.9.5 - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K445[m[K51.txt

FrontAccounting 1.13 - Remote File Inclusion
| php/webapps/[01;31m[K445[m[K6.txt
```

FTP Client 0.17-19build1 ACCT (Ubuntu 10.04) - Buffer Overflow (PoC)
| linux/dos/1[01;31m[K445[m[K2.txt

FTPShell Client 6.7 - Buffer Overflow
| windows/remote/[01;31m[K445[m[K96.py

gif2apng 1.9 - '.gif' Stack Buffer Overflow
| linux/dos/[01;31m[K445[m[K19.txt

GitList 0.6 - Remote Code Execution
| php/webapps/[01;31m[K445[m[K48.py

glossword 1.8.12 - Multiple Vulnerabilities
| php/webapps/2[01;31m[K445[m[K6.txt

Glossword 1.8.3 - SQL Injection
| php/webapps/2[01;31m[K445[m[K7.txt

GNU Beep 1.3 - 'HoleyBeep' Local Privilege Escalation
| linux/local/4[01;31m[K445[m[K2.py

Google Chrome V8 - Object Allocation Size Integer Overflow
| multiple/remote/[01;31m[K445[m[K84.txt

GPON Routers - Authentication Bypass / Command Injection
| hardware/remote/[01;31m[K445[m[K76.sh

Hanso Player 2.5.0 - 'm3u' Buffer Overflow (Denial of Service)
| windows/dos/29[01;31m[K445[m[K.rb

HP OpenView Network Node Manager (OV NNM) 7.5.1 - 'ovalarmsrv.exe'
Remote Overflow |
windows/remote/5[01;31m[K445[m[K.cpp

HRSALE The Ultimate HRM 1.0.2 - 'award_id' SQL Injection
| php/webapps/[01;31m[K445[m[K37.txt

HRSALE The Ultimate HRM 1.0.2 - (Authenticated) Cross-Site Scripting
| php/webapps/[01;31m[K445[m[K38.txt

HRSALE The Ultimate HRM 1.0.2 - CSV Injection
| php/webapps/[01;31m[K445[m[K36.txt

HRSALE The Ultimate HRM 1.0.2 - Local File Inclusion
| php/webapps/[01;31m[K445[m[K39.txt

HWiNFO 5.82-3410 - Denial of Service
| windows/dos/[01;31m[K445[m[K93.py

IBM AIX 5l - 'FTPd' Remote DES Hash
| aix/remote/1[01;31m[K445[m[K6.c

```
IceWarp Mail Server < 11.1.1 - Directory Traversal
| php/webapps/[01;31m[K445[m[K87.txt

Interspire Email Marketer < 6.1.6 - Remote Admin Authentication Bypass
| php/webapps/[01;31m[K445[m[K13.py

JBoard - Multiple Cross-Site Scripting / SQL Injections
| php/webapps/3[01;31m[K445[m[K6.txt

Jfrog Artifactory < 4.16 - Arbitrary File Upload / Remote Command
Execution                                |
linux/webapps/[01;31m[K445[m[K43.txt

Joomla! Component com_iproperty - SQL Injection
| php/webapps/1[01;31m[K445[m[K0.txt

Joomla! Component com_realestatemanager 3.7 - SQL Injection
| php/webapps/38[01;31m[K445[m[K.txt

Joomla! Component JO Facebook Gallery 4.5 - SQL Injection
| php/webapps/41[01;31m[K445[m[K.txt

Joomla! Component Tour de France Pool 1.0.1 Module -
MosConfig_absolute_path Remote File Inclusion         |
php/webapps/30[01;31m[K445[m[K.txt

JTL-Shop 2 - 'druckansicht.php' SQL Injection
| php/webapps/11[01;31m[K445[m[K.txt

Kartris 1.6 - Arbitrary File Upload
| aspx/webapps/48[01;31m[K445[m[K.txt

Kaspersky KSN for Linux 5.2 - Memory Corruption
| linux/dos/[01;31m[K445[m[K21.py

kic 2.4a - Denial of Service
| linux/dos/47[01;31m[K445[m[K.py

lastore-daemon D-Bus - Privilege Escalation (Metasploit)
| linux/local/[01;31m[K445[m[K23.rb

LibreOffice/Open Office - '.odt' Information Disclosure
| windows/local/[01;31m[K445[m[K64.py

Linux Kernel 2.6.32-5 (Debian 6.0.5) - '/dev/ptmx' Key Stroke Timing
Local Disclosure                      |
linux/local/2[01;31m[K445[m[K9.sh

Linux Kernel < 4.17-rc1 - 'AF_LLC' Double Free
| linux/dos/[01;31m[K445[m[K79.c

LiveStreet 0.2 - Comment Topic Header Cross-Site Scripting
| php/webapps/34[01;31m[K445[m[K.txt
```

```
Metasploit Framework - 'msfd' Remote Code Execution (Metasploit)
| ruby/remote/[01;31m[K445[m[K70.rb

Metasploit Framework - 'msfd' Remote Code Execution (via Browser)
(Metasploit)                                |
ruby/remote/[01;31m[K445[m[K69.rb

Microsoft Credential Security Support Provider - Remote Code Execution
| windows/remote/4[01;31m[K445[m[K3.md

Microsoft Edge 38.14393.1066.0 - 'textarea.defaultValue' Memory
Disclosure                                  | windows_x86-
64/dos/42[01;31m[K445[m[K.html

Microsoft FrontPage Personal Web Server 1.0 - PWS Denial of Service
| windows/dos/19[01;31m[K445[m[K.txt

Microsoft IIS 1.0 / Netscape Server 1.0/1.12 / OReilly WebSite
Professional 1.1b - '.cmd' / '.CMD' Remote  |
windows/remote/20[01;31m[K445[m[K.txt

Microsoft Internet Explorer - Memory Corruption (PoC) (MS14-029)
| windows/dos/3[01;31m[K445[m[K8.html

Microsoft Internet Explorer 11.371.16299.0 (Windows 10) - Denial Of
Service                                     |
windows/dos/[01;31m[K445[m[K25.py

Microsoft Windows - 'nt!NtQueryAttributesFile' Kernel Stack Memory
Disclosure                                  |
windows/dos/4[01;31m[K445[m[K9.cpp

Microsoft Windows - 'nt!NtQueryFullAttributesFile' Kernel Stack Memory
Disclosure                                  |
windows/dos/4[01;31m[K445[m[K8.cpp

Microsoft Windows - Local Privilege Escalation
| windows/local/[01;31m[K445[m[K81.c

Microsoft Windows Media Player - '.mid' Integer Overflow (PoC)
| windows/dos/8[01;31m[K445[m[K.pl

Microsoft Windows WMI - Recieve Notification Exploit (Metasploit)
| windows_x86-64/local/[01;31m[K445[m[K86.rb

MikroTik 6.41.4 - FTP daemon Denial of Service (PoC)
| linux/dos/4[01;31m[K445[m[K0.txt

Monstra CMS 3.0.4 - Arbitrary Folder Deletion
| php/webapps/[01;31m[K445[m[K12.txt

Monstra cms 3.0.4 - Persitent Cross-Site Scripting
| php/webapps/[01;31m[K445[m[K02.txt
```

```
Motorola Timbuktu Pro 8.6.5 - File Deletion/Creation
| windows/remote/[01;31m[K445[m[K5.pl

MusicBox 2.3 - 'index.php' SQL Injection
| php/webapps/27[01;31m[K445[m[K.txt

MyBB Threads to Link Plugin 1.3 - Cross-Site Scripting
| php/webapps/[01;31m[K445[m[K47.txt

MySQL 5 - Command Line Client HTML Special Characters HTML Injection
| linux/remote/32[01;31m[K445[m[K.txt

Nagios XI 5.2.6 < 5.2.9 / 5.3 / 5.4 - Chained Remote Root
| php/webapps/[01;31m[K445[m[K60.py

Navicat < 12.0.27 - Oracle Connection Overflow
| windows/dos/[01;31m[K445[m[K58.py

NaviCOPA Web Server 2.01 - 'GET' Remote Buffer Overflow
| windows/remote/2[01;31m[K445[m[K.c

Navigate CMS 2.8 - Cross-Site Scripting
| php/webapps/45[01;31m[K445[m[K.txt

Norton Core Secure WiFi Router - 'BLE' Command Injection (PoC)
| hardware/remote/[01;31m[K445[m[K74.txt

Novus 1.0 - 'notas.asp?nota_id' SQL Injection
| asp/webapps/[01;31m[K445[m[K8.txt

NTPd ntp-4.2.6p5 - 'ctl_putdata()' Buffer Overflow (PoC)
| linux/dos/39[01;31m[K445[m[K.c

October CMS User Plugin 1.4.5 - Persistent Cross-Site Scripting
| php/webapps/[01;31m[K445[m[K46.txt

Open Realty 2.x/3.x - Persistent Cross-Site Scripting
| php/webapps/1[01;31m[K445[m[K9.txt

Open-AudIT 2.1 - CSV Macro Injection
| windows/webapps/[01;31m[K445[m[K11.txt

OpenLDAP 2.4.x - 'modrdn' NULL OldDN Remote Denial of Service
| linux/dos/35[01;31m[K445[m[K.txt

Oracle Automated Service Manager 1.3 - Installation Privilege
Escalation                                    |
linux/local/2[01;31m[K445[m[K8.txt

Oracle Weblogic Server 10.3.6.0 / 12.1.3.0 / 12.2.1.2 / 12.2.1.3 -
Deserialization Remote Command Executio |
multiple/remote/[01;31m[K445[m[K53.py
```

```
osCommerce 2.2 - 'osCsid' Cross-Site Scripting
| php/webapps/23[01;31m[K445[m[K.txt

Palo Alto Networks - 'readSessionVarsFromFile()' Session Corruption
(Metasploit)                              |
unix/remote/[01;31m[K445[m[K97.rb

PaoBacheca 2.1 - 'index.php' URI Cross-Site Scripting
| php/webapps/3[01;31m[K445[m[K3.txt

PaoBacheca 2.1 - 'scrivi.php' URI Cross-Site Scripting
| php/webapps/3[01;31m[K445[m[K4.txt

PhotoPost PHP 4.6.5 - 'ecard.php' SQL Injection
| php/webapps/1[01;31m[K445[m[K3.txt

PHPInstantGallery 1.1 - 'admin.php' Cross-Site Scripting
| php/webapps/33[01;31m[K445[m[K.txt

PhpWiki - Remote Command Execution
| php/webapps/3[01;31m[K445[m[K1.py

PlaySMS - 'import.php' (Authenticated) CSV File Upload Code Execution
(Metasploit)                          | php/remote/[01;31m[K445[m[K98.rb

PlaySMS 1.4 - 'sendfromfile.php?Filename' (Authenticated) 'Code
Execution (Metasploit)                     |
php/remote/[01;31m[K445[m[K99.rb

Portable UPnP SDK - 'unique_service_name()' Remote Code Execution
(Metasploit)                                |
unix/remote/2[01;31m[K445[m[K5.rb

PRTG Network Monitor < 18.1.39.1648 - Stack Overflow (Denial of
Service)                                     |
windows_x86/dos/[01;31m[K445[m[K00.py

RealityServer Web Services RTMP Server 3.1.1 build
1[01;31m[K445[m[K25.5 - Null Pointer Dereference Denial of Service   |
windows/dos/35895.txt

RealNetworks GameHouse 'InstallerDlg.dll' 2.6.0.[01;31m[K445[m[K
ActiveX Control - Multiple Vulnerabilities             |
windows/remote/35560.txt

RGui 3.4.4 - Local Buffer Overflow
| windows/local/[01;31m[K445[m[K16.py

Rock Band CMS 0.10 - 'news.php' Multiple SQL Injections (2)
| php/webapps/3[01;31m[K445[m[K5.txt

SAP SOAP RFC - SXPG_CALL_SYSTEM Remote Command Execution (Metasploit)
| multiple/remote/25[01;31m[K445[m[K.rb
```

Schneider Electric InduSoft Web Studio and InTouch Machine Edition - Denial of Service | windows/dos/[01;31m[K445[m[K72.txt

ScozBook 1.1 - Full Path Disclosure | php/webapps/22[01;31m[K445[m[K.txt

Shopy Point of Sale 1.0 - CSV Injection | php/webapps/[01;31m[K445[m[K34.txt

SickRage < v2018.03.09 - Clear-Text Credentials HTTP Response | linux/webapps/[01;31m[K445[m[K45.py

Simple Machine Forum 2.0.x < 2.0.4 - File Disclosure / Directory Traversal | php/webapps/24[01;31m[K445[m[K.txt

sk.log 0.5.3 - 'skin_url' Remote File Inclusion | php/webapps/[01;31m[K445[m[K4.txt

SkaLinks 1.5 - 'register.php' Arbitrary Add Editor | php/webapps/6[01;31m[K445[m[K.txt

sNews - 'index.php' SQL Injection | php/webapps/1[01;31m[K445[m[K8.txt

Sniper Elite 1.0 - Null Pointer Dereference Denial of Service | multiple/dos/3[01;31m[K445[m[K7.txt

Snitz Forums 2000 < 3.4.0.3 - Multiple Vulnerabilities | multiple/webapps/43[01;31m[K445[m[K.txt

Softbiz Classifieds PLUS - 'id' SQL Injection | php/webapps/[01;31m[K445[m[K7.txt

SysGauge Pro 4.6.12 - Local Buffer Overflow (SEH) | windows/local/4[01;31m[K445[m[K5.py

TBK DVR4104 / DVR4216 - Credentials Leak | hardware/remote/[01;31m[K445[m[K77.py

Tender System 0.9.5b - Local File Inclusion | php/webapps/10[01;31m[K445[m[K.txt

TP-Link Technologies TL-WA850RE Wi-Fi Range Extender - Remote Reboot | hardware/webapps/[01;31m[K445[m[K50.txt

UK Cookie Consent - Persistent Cross-Site Scripting | php/webapps/[01;31m[K445[m[K03.txt

ValidForm Builder script - Remote Command Execution | php/webapps/1[01;31m[K445[m[K4.txt

```
vBulletin 3.8.6 - 'faq.php' Information Disclosure
| php/webapps/1[01;31m[K445[m[K5.txt

VLC Media Player/Kodi/PopcornTime 'Red Chimera' < 2.2.5 - Memory
Corruption (PoC)                              |
windows/dos/[01;31m[K445[m[K14.py

VMware Workstation 12.5.2 - Drag n Drop Use-After-Free (Pwn2Own 2017)
(PoC)                                  | windows/dos/[01;31m[K445[m[K33.c

Voting System 1.0 - File Upload RCE (Authenticated Remote Code
Execution)                                     |
php/webapps/49[01;31m[K445[m[K.py

WebKit - 'WebCore::jsElementScrollHeightGetter' Use-After-Free
| multiple/dos/[01;31m[K445[m[K66.html

Websphere/JBoss/OpenNMS/Symantec Endpoint Protection Manager - Java
Deserialization Remote Code Execution  |
multiple/remote/[01;31m[K445[m[K52.sh

WordPress Plugin Backup Migration 1.2.8 - Unauthenticated Database
Backup                                       |
php/webapps/51[01;31m[K445[m[K.txt

WordPress Plugin Form Maker 1.12.20 - CSV Injection
| php/webapps/[01;31m[K445[m[K59.txt

WordPress Plugin Responsive Cookie Consent 1.7 / 1.6 / 1.5 -
(Authenticated) Persistent Cross-Site Scripti |
php/webapps/[01;31m[K445[m[K63.txt

WordPress Plugin The Welcomizer 1.3.9.4 - 'twiz-index.php' Cross-Site
Scripting                                  |
php/webapps/36[01;31m[K445[m[K.txt

WordPress Plugin User Role Editor < 4.25 - Privilege Escalation
| php/webapps/[01;31m[K445[m[K95.rb

WordPress Plugin WF Cookie Consent 1.1.3 - Cross-Site Scripting
| php/webapps/[01;31m[K445[m[K85.txt

WordPress Plugin Woo Import Export 1.0 - Arbitrary File Deletion
| php/webapps/[01;31m[K445[m[K20.html

WordPress Plugin WP with Spritz 1.0 - Remote File Inclusion
| php/webapps/[01;31m[K445[m[K44.php

WSO2 Carbon / WSO2 Dashboard Server 5.3.0 - Persistent Cross-Site
Scripting                                       |
java/webapps/[01;31m[K445[m[K31.txt
```

```
WUZHI CMS 4.1.0 - Cross-Site Request Forgery
| php/webapps/[01;31m[K445[m[K04.txt

xdebug < 2.5.5 - OS Command Execution (Metasploit)
| php/remote/[01;31m[K445[m[K68.rb

Xitami Web Server 2.5 - 'If-Modified-Since' Remote Buffer Overflow
| windows/remote/[01;31m[K445[m[K0.py

XRms - Blind SQL Injection / Command Execution
| php/webapps/3[01;31m[K445[m[K2.py

ZeeMatri 3.x - Arbitrary File Upload
| php/webapps/14[01;31m[K445[m[K.txt

---------------------------------------------------------------------------------------- ----------------
----------

---------------------------------------------------------------------------------------- ----------------
----------
Shellcode Title
|  Path

---------------------------------------------------------------------------------------- ----------------
----------
Linux/x64 - execve() Assembly Shellcode (Generator)
| generator/44[01;31m[K445[m[K.py

Linux/x86 - Bind (1337/TCP) Shell (/bin/sh) + Null-Free Shellcode (92
bytes)                                | linux_x86/[01;31m[K445[m[K05.c

Linux/x86 - chmod 4755 /bin/dash Shellcode (33 bytes)
| linux_x86/[01;31m[K445[m[K09.c

Linux/x86 - Edit /etc/sudoers (ALL ALL=(ALL) NOPASSWD: ALL) For Full
Access + Null-Free Shellcode (79 byte | linux_x86/[01;31m[K445[m[K07.c

Linux/x86 - execve(/bin/sh) + NOT Encoded Shellcode (27 bytes)
| linux_x86/[01;31m[K445[m[K94.c

Linux/x86 - execve(/bin/sh) + ROT-13/RShift-2/XOR Encoded Shellcode (44
bytes)                              | linux_x86/[01;31m[K445[m[K17.c

Linux/x86 - execve(/bin/sh) Shellcode (38 bytes)
| linux_x86/13[01;31m[K445[m[K.c

Linux/x86 - execve(cp /bin/sh /tmp/sh; chmod +s /tmp/sh) + Null-Free
Shellcode (74 bytes)                  | linux_x86/[01;31m[K445[m[K10.c

Linux/x86 - Reverse (127.1.1.1:5555/TCP) Shell Shellcode (73 Bytes)
| linux_x86/[01;31m[K445[m[K08.c
```

Windows/x86 (XP SP3) - Add Firewall Rule (Allow [01;31m[K445[m[K/TCP) Shellcode | windows_x86/13569.asm

---

Port: 513

Exploit Title | Path

ActFax 10.10 - Unquoted Path Services | windows/local/[01;31m[K513[m[K32.txt

Adobe Connect 11.4.5 - Local File Disclosure | multiple/webapps/[01;31m[K513[m[K27.txt

ae2 - 'standart.inc.php' Remote File Inclusion | php/webapps/2[01;31m[K513[m[K.txt

AgataSoft Auto PingMaster 1.5 - 'Host name' Denial of Service (PoC) | windows/dos/4[01;31m[K513[m[K7.py

Agilebio Lab Collector Electronic Lab Notebook v4.234 - Remote Code Execution (RCE) | php/webapps/[01;31m[K513[m[K07.py

Altenergy Power Control Software C1.2.5 - OS command injection | hardware/webapps/[01;31m[K513[m[K25.py

Android - Hardware Service Manager Arbitrary Service Replacement due to getpidcon | android/dos/43[01;31m[K513[m[K.txt

Apache James Server 2.3.2 - Remote Command Execution | linux/remote/35[01;31m[K513[m[K.py

Arachni Web Application Scanner Web UI - Persistent Cross-Site Scripting | multiple/webapps/34[01;31m[K513[m[K.txt

Arcsoft PhotoStudio 6.0.0.172 - Unquoted Service Path | windows/local/[01;31m[K513[m[K93.txt

AspEmail v5.6.0.2 - Local Privilege Escalation | windows/local/[01;31m[K513[m[K80.txt

ASUS DSL-N12E_C1 1.1.2.3_345 - Remote Command Execution
| hardware/webapps/4[01;31m[K513[m[K5.txt

Athena Web Registration - Remote Command Execution
| php/webapps/23[01;31m[K513[m[K.txt

AtomatiCMS - Upload Arbitrary File
| asp/webapps/1[01;31m[K513[m[K9.txt

AuraCMS 1.62 - Multiple SQL Injections
| php/webapps/[01;31m[K513[m[K0.py

Bang Resto v1.0 - 'Multiple' SQL Injection
| php/webapps/[01;31m[K513[m[K78.txt

Bang Resto v1.0 - Stored Cross-Site Scripting (XSS)
| php/webapps/[01;31m[K513[m[K77.txt

Barracuda Networks Spam & Virus Firewall 4.1.1.021 - Remote
Configuration Retrieval |
cgi/webapps/1[01;31m[K513[m[K0.sh

Barracuda SSL VPN - 'fileSystem.do' Multiple Cross-Site Scripting
Vulnerabilities |
hardware/remote/37[01;31m[K513[m[K.txt

Bludit 4.0.0-rc-2 - Account takeover
| php/webapps/[01;31m[K513[m[K60.txt

Blue Coat Authentication and Authorization Agent (BCAAA) 5 - Remote
Buffer Overflow (Metasploit) |
windows/remote/17[01;31m[K513[m[K.rb

Bontago Game Server 1.1 - Remote Nickname Buffer Overrun
| multiple/remote/2[01;31m[K513[m[K2.txt

BrainyCP V1.0 - Remote Code Execution
| php/webapps/[01;31m[K513[m[K57.py

BXCP 0.2.9.9 - 'tid' SQL Injection
| php/webapps/1[01;31m[K513[m[K.php

Calendar Script 1.1 - Insecure Cookie Handling
| php/webapps/7[01;31m[K513[m[K.txt

Calibre 0.7.34 - Cross-Site Scripting / Directory Traversal
| windows/remote/3[01;31m[K513[m[K0.txt

Car Portal 2.0 - Blind SQL Injection
| php/webapps/1[01;31m[K513[m[K5.txt

CartWIZ 1.10 - 'AddToWishlist.asp' Cross-Site Scripting
| asp/webapps/25[01;31m[K513[m[K.txt

```
Chitor-CMS v1.1.2 - Pre-Auth SQL Injection
| php/webapps/[01;31m[K513[m[K83.py

ChurchCRM 4.5.1 - Authenticated SQL Injection
| php/webapps/[01;31m[K513[m[K19.py

CoSoSys Endpoint Protector 4.5.0.1 - (Authenticated) Remote Root
Command Injection                          |
php/webapps/4[01;31m[K513[m[K1.py

craftercms 4.x.x - CORS
| multiple/webapps/[01;31m[K513[m[K13.txt

D-Link IP Cameras - Multiple Vulnerabilities
| hardware/webapps/2[01;31m[K513[m[K8.txt

DFLabs PTK 1.0.5 - Steal Authentication Credentials
| php/webapps/18[01;31m[K513[m[K.txt

Digital Music Pad 8.2.3.3.4 - Local Overflow (SEH) (Metasploit)
| windows/local/1[01;31m[K513[m[K4.rb

Docker based datastores for IBM Instana 241-2 243-0 - No Authentication
| multiple/remote/[01;31m[K513[m[K14.py

Dokeos Lms 1.8.5 - 'Include' Remote Code Execution
| php/webapps/8[01;31m[K513[m[K.pl

dotclear 2.25.3 - Remote Code Execution (RCE) (Authenticated)
| php/webapps/[01;31m[K513[m[K53.txt

Eicon Networks DIVA LAN ISDN Modem 1.0 Release 2.5/1.0/2.0 - Denial of
Service                                    |
hardware/dos/19[01;31m[K513[m[K.txt

ENTAB ERP 1.0 - Username PII leak
| asp/webapps/[01;31m[K513[m[K35.txt

Entrepreneur Bus Booking Script 3.03 - 'hid_Busid' SQL Injection
| php/webapps/41[01;31m[K513[m[K.txt

Epic Games Unreal Engine Logging Function - Remote Denial of Service
| multiple/dos/30[01;31m[K513[m[K.txt

ESET Service 16.0.26.0 - 'Service ekrn' Unquoted Service Path
| windows/local/[01;31m[K513[m[K51.txt

Esotalk CMS 1.0.0g4 - Cross-Site Scripting
| php/webapps/3[01;31m[K513[m[K8.txt

ever gauzy v0.281.9 - JWT weak HMAC secret
| typescript/webapps/[01;31m[K513[m[K54.txt
```

```
File Replication Pro 7.5.0 - Privilege Escalation/Password reset due
Incorrect Access Control              |
windows/local/[01;31m[K513[m[K75.txt

Flippa Marketplace Clone 1.0 - 'date_started' SQL Injection
| php/webapps/45[01;31m[K513[m[K.txt

FormaLMS 2.4.4 - Authentication Bypass
| multiple/webapps/50[01;31m[K513[m[K.py

FortiRecorder 6.4.3 - Denial of Service
| hardware/dos/[01;31m[K513[m[K26.py

Fox Audio Player 0.8.0 - '.m3u' Denial of Service
| windows/dos/1[01;31m[K513[m[K1.txt

Franklin Fueling Systems  TS-550 - Exploit and Default Password
| hardware/remote/[01;31m[K513[m[K21.txt

Franklin Fueling Systems TS-550 - Default Password
| hardware/remote/[01;31m[K513[m[K82.txt

FUXA V.1.1.13-1186 - Unauthenticated Remote Code Execution (RCE)
| typescript/webapps/[01;31m[K513[m[K85.txt

FuzeZip 1.0.0.131625 - Local Buffer Overflow (SEH)
| windows/local/2[01;31m[K513[m[K0.py

GDidees CMS 3.9.1 - Local File Disclosure
| php/webapps/[01;31m[K513[m[K81.txt

Goanywhere Encryption helper 7.1.1 - Remote Code Execution (RCE)
| java/webapps/[01;31m[K513[m[K39.java

Google Chrome  109.0.5414.74 - Code Execution via missing lib file
(Ubuntu)                                |
linux/local/[01;31m[K513[m[K31.txt

Google Chrome Browser 111.0.5563.64 - AXPlatformNodeCocoa Fatal
OOM/Crash (macOS)                         |
macos/local/[01;31m[K513[m[K61.txt

Haihaisoft HUPlayer 1.0.4.8 - '.m3u' / '.pls' / '.asx' Buffer Overflow
(SEH)                               | windows/dos/32[01;31m[K513[m[K.py

HospitalRun  1.0.0-beta - Local Root Exploit for macOS
| macos/local/[01;31m[K513[m[K10.rb

IBM Aspera Faspex 4.4.1 - YAML deserialization (RCE)
| multiple/remote/[01;31m[K513[m[K16.py

iCat Electronic Commerce Suite 3.0 - File Disclosure
| multiple/remote/20[01;31m[K513[m[K.txt
```

```
Icinga Web 2.10 - Arbitrary File Disclosure
| php/webapps/[01;31m[K513[m[K29.py

Imperva SecureSphere 11.5 / 12.0 / 13.0 - Privilege Escalation
| linux/local/4[01;31m[K513[m[K0.py

ImpressCMS 1.2.x - 'quicksearch_ContentContent' HTML Injection
| php/webapps/3[01;31m[K513[m[K4.txt

InnovaStudio WYSIWYG Editor 5.4 - Unrestricted File Upload / Directory
Traversal                           |
asp/webapps/[01;31m[K513[m[K62.txt

Interspire Email Marketer < 6.1.6 - Remote Admin Authentication Bypass
| php/webapps/44[01;31m[K513[m[K.py

IpTools 0.1.4 - Tiny TCP/IP servers Directory Traversal
| windows/remote/36[01;31m[K513[m[K.txt

IPUX CL5452/CL[01;31m[K513[m[K2 IP Camera - 'UltraSVCamX.ocx' ActiveX
Stack Buffer Overflow                               |
hardware/remote/35421.txt

iTech Multi Vendor Script 6.63 - SQL Injection
| php/webapps/42[01;31m[K513[m[K.txt

iworkstation 9.3.2.1.4 - Local Overflow (SEH)
| windows/local/1[01;31m[K513[m[K3.pl

Joomla! Component astatsPRO 1.0 - 'refer.php' SQL Injection
| php/webapps/[01;31m[K513[m[K8.txt

Joomla! Component Classified - SQL Injection
| php/webapps/3[01;31m[K513[m[K5.txt

Joomla! Component com_galeria - SQL Injection
| php/webapps/[01;31m[K513[m[K4.txt

Joomla! Component jooget 2.6.8 - SQL Injection
| php/webapps/[01;31m[K513[m[K2.txt

Joomla! v4.2.8 - Unauthenticated information disclosure
| php/webapps/[01;31m[K513[m[K34.py

Katalog Plyt Audio (pl) 1.0 - SQL Injection
| php/webapps/3[01;31m[K513[m[K.php

KodExplorer 4.49 - CSRF to Arbitrary File Upload
| php/webapps/[01;31m[K513[m[K88.py

Lilac-Reloaded for Nagios 2.0.8 - Remote Code Execution (RCE)
| php/webapps/[01;31m[K513[m[K74.py
```

Linux Kernel 2.6.31-rc7 - 'AF_LLC getsockname' 5-Byte Stack Disclosure
| linux/local/9[01;31m[K513[m[K.c

Linux Kernel 6.2 - Userspace Processes To Enable Mitigation
| linux/local/[01;31m[K513[m[K84.txt

Lucee Scheduled Job v1.0 - Command Execution
| multiple/local/[01;31m[K513[m[K33.rb

MAC 1200R - Directory Traversal
| hardware/webapps/[01;31m[K513[m[K15.txt

Mambo Component Portfolio Manager 1.0 - 'categoryId' SQL Injection
| php/webapps/[01;31m[K513[m[K9.txt

Mambo Component Ricette 1.0 - SQL Injection
| php/webapps/[01;31m[K513[m[K3.txt

Mars Stealer 8.3 - Admin Account Takeover
| php/webapps/[01;31m[K513[m[K92.py

Medicine Tracker System v1.0 - Sql Injection
| php/webapps/[01;31m[K513[m[K38.txt

MetaForum 0.[01;31m[K513[m[K Beta - Arbitrary File Upload
| php/webapps/3516.php

Microsoft Edge (Chromium-based) Webview2 1.0.1661.34 - Spoofing
| multiple/local/[01;31m[K513[m[K59.txt

Microsoft Excel 365 MSO (Version 2302 Build 16.0.16130.20186) 64-bit -
Remote Code Execution (RCE) |
multiple/remote/[01;31m[K513[m[K28.txt

Microsoft Word 16.72.23040900 - Remote Code Execution (RCE)
| multiple/remote/[01;31m[K513[m[K76.txt

Mitel Audio and Web Conferencing (AWC) - Arbitrary Shell Command
Injection |
linux/remote/3[01;31m[K513[m[K2.txt

Mitel MiCollab AWV 8.1.2.4 and 9.1.3 - Directory Traversal and LFI
| cgi/webapps/[01;31m[K513[m[K08.txt

MPCSoftWeb 1.0 - Database Disclosure
| asp/webapps/22[01;31m[K513[m[K.txt

Multi-Vendor Online Groceries Management System 1.0 - Remote Code
Execution |
php/webapps/[01;31m[K513[m[K94.py

Netgear DGN2200B - Multiple Vulnerabilities
| hardware/webapps/24[01;31m[K513[m[K.txt

NotrinosERP 0.7 - Authenticated Blind SQL Injection
| php/webapps/[01;31m[K513[m[K18.py

OCS Inventory NG 2.3.0.0 - Unquoted Service Path
| windows/local/[01;31m[K513[m[K89.txt

ODFaq 2.1.0 - Blind SQL Injection
| php/webapps/5[01;31m[K513[m[K.pl

Online Appointment System V1.0 - Cross-Site Scripting (XSS)
| php/webapps/[01;31m[K513[m[K37.txt

Online Computer and Laptop Store 1.0 - Remote Code Execution (RCE)
| php/webapps/[01;31m[K513[m[K58.py

Online-Pizza-Ordering -1.0 - Remote Code Execution (RCE)
| php/webapps/[01;31m[K513[m[K44.txt

OpenCimetiere 3.0.0-a5 - Blind SQL Injection
| php/webapps/40[01;31m[K513[m[K.txt

Oracle Weblogic Server - Deserialization Remote Command Execution
(Patch Bypass) |
multiple/remote/46[01;31m[K513[m[K.java

Osprey Pump Controller 1.0.1 - (eventFileSelected) Command Injection
| hardware/remote/[01;31m[K513[m[K06.txt

Osprey Pump Controller 1.0.1 - (pseudonym) Semi-blind Command Injection
| hardware/remote/[01;31m[K513[m[K00.txt

Osprey Pump Controller 1.0.1 - (userName) Blind Command Injection
| hardware/remote/[01;31m[K513[m[K01.txt

Osprey Pump Controller 1.0.1 - Authentication Bypass Credentials
Modification |
hardware/remote/[01;31m[K513[m[K03.py

Osprey Pump Controller 1.0.1 - Cross-Site Request Forgery
| hardware/remote/[01;31m[K513[m[K04.txt

Osprey Pump Controller 1.0.1 - Unauthenticated Remote Code Execution
Exploit |
hardware/remote/[01;31m[K513[m[K05.py

Osprey Pump Controller v1.0.1 - Unauthenticated Reflected XSS
| hardware/remote/[01;31m[K513[m[K02.txt

Palo Alto Cortex XSOAR 6.5.0 - Stored Cross-Site Scripting (XSS)
| multiple/webapps/[01;31m[K513[m[K43.txt

PaperCut NG/MG 22.0.4 - Authentication Bypass
| multiple/webapps/[01;31m[K513[m[K91.py

```
Paradox Security Systems IPR512 - Denial Of Service
| hardware/dos/[01;31m[K513[m[K56.sh

Paul Smith Computer Services VCAP Calendar Server 1.9 - Remote Denial
of Service                              |
windows/dos/28[01;31m[K513[m[K.txt

Pentaho BA Server EE 9.3.0.0-428 - Remote Code Execution (RCE)
(Unauthenticated)                         |
jsp/webapps/[01;31m[K513[m[K50.txt

pfsenseCE v2.6.0 - Anti-brute force protection bypass
| hardware/remote/[01;31m[K513[m[K52.py

PHP Restaurants 1.0 - SQLi Authentication Bypass & Cross Site Scripting
| php/webapps/[01;31m[K513[m[K98.txt

PHP-Stats 0.1.9.2 - Multiple Vulnerabilities
| php/webapps/4[01;31m[K513[m[K.php

PHPizabi 0.848b C1 HFP1 - Arbitrary File Upload
| php/webapps/[01;31m[K513[m[K6.txt

phpMyAdmin - 'preg_replace' (Authenticated) Remote Code Execution
(Metasploit)                              |
php/remote/2[01;31m[K513[m[K6.rb

phpMyFAQ v3.1.12 - CSV Injection
| php/webapps/[01;31m[K513[m[K99.txt

PHPWCMS 1.2.5 -DEV - 'imgdir' Traversal Arbitrary File Access
| php/webapps/26[01;31m[K513[m[K.txt

Piwigo 13.6.0 - Stored Cross-Site Scripting (XSS)
| php/webapps/[01;31m[K513[m[K86.txt

Plesk/myLittleAdmin - ViewState .NET Deserialization (Metasploit)
| windows/remote/48[01;31m[K513[m[K.rb

ProjeQtOr Project Management System 10.3.2 - Remote Code Execution
(RCE)                                     |
php/webapps/[01;31m[K513[m[K87.txt

Purchase Order Management-1.0 - Local File Inclusion
| php/webapps/[01;31m[K513[m[K12.txt

Quick Classifieds 1.0 - 'include/usersHead.inc?DOCUMENT_ROOT' Remote
File Inclusion                          |
php/webapps/31[01;31m[K513[m[K.txt

Restaurant Management System 1.0  - SQL Injection
| php/webapps/[01;31m[K513[m[K30.txt
```

```
Rianxosencabos CMS 0.9 - Arbitrary Add Admin
| php/webapps/6[01;31m[K513[m[K.txt

Roxy Fileman 1.4.5 -  Arbitrary File Upload
| ashx/webapps/[01;31m[K513[m[K55.txt

RSA NetWitness Platform 12.2 - Incorrect Access Control / Code
Execution                                    |
windows/local/[01;31m[K513[m[K36.txt

Rukovoditel 3.3.1 - Remote Code Execution (RCE)
| php/webapps/[01;31m[K513[m[K22.txt

Sales Tracker Management System v1.0 - Multiple Vulnerabilities
| php/webapps/51[01;31m[K513[m[K.txt

Schneider Electric v1.0 - Directory traversal & Broken Authentication
| hardware/remote/[01;31m[K513[m[K20.txt

SecureSphere 12.0.0.50 - SealMode Shell Escape (Metasploit)
| linux/local/4[01;31m[K513[m[K2.rb

Seq 4.2.476 - Authentication Bypass
| windows/webapps/4[01;31m[K513[m[K6.py

Serendipity 2.4.0 - Cross-Site Scripting (XSS)
| php/webapps/[01;31m[K513[m[K73.txt

Serendipity 2.4.0 - Remote Code Execution (RCE) (Authenticated)
| php/webapps/[01;31m[K513[m[K72.txt

Sielco Analog FM Transmitter 2.12 - 'id' Cookie Brute Force Session
Hijacking                                  |
hardware/webapps/[01;31m[K513[m[K63.txt

Sielco Analog FM Transmitter 2.12 - Cross-Site Request Forgery
| hardware/webapps/[01;31m[K513[m[K64.txt

Sielco Analog FM Transmitter 2.12 - Improper Access Control Change
Admin Password                             |
hardware/webapps/[01;31m[K513[m[K65.txt

Sielco Analog FM Transmitter 2.12 - Remote Privilege Escalation
| hardware/remote/[01;31m[K513[m[K66.txt

Sielco PolyEco Digital FM Transmitter 2.0.6 - Account Takeover /
Lockout / EoP                               |
hardware/webapps/[01;31m[K513[m[K71.txt

Sielco PolyEco Digital FM Transmitter 2.0.6 - Authentication Bypass
Exploit                                    |
hardware/webapps/[01;31m[K513[m[K67.py
```

Sielco PolyEco Digital FM Transmitter 2.0.6 - Authorization Bypass Factory Reset | hardware/webapps/[01;31m[K513[m[K68.txt

Sielco PolyEco Digital FM Transmitter 2.0.6 - Radio Data System POST Manipulation | hardware/webapps/[01;31m[K513[m[K69.txt

Sielco PolyEco Digital FM Transmitter 2.0.6 - Unauthenticated Information Disclosure | hardware/webapps/[01;31m[K513[m[K70.txt

Simple CMS 1.0.3 - 'area' SQL Injection | php/webapps/[01;31m[K513[m[K1.pl

Sitecore Staging Module 5.4.0 - Authentication Bypass / File Manipulation | windows/webapps/10[01;31m[K513[m[K.txt

Snitz Forum v1.0 - Blind SQL Injection | asp/webapps/[01;31m[K513[m[K23.txt

Social Share - 'Username' SQL Injection | php/webapps/3[01;31m[K513[m[K1.txt

Social Share - 'vote.php' HTTP Response Splitting | php/webapps/3[01;31m[K513[m[K7.txt

Sophos Web Appliance 4.3.10.4 - Pre-auth command injection | php/webapps/[01;31m[K513[m[K96.sh

Stonesoft VPN Client 6.2.0 / 6.8.0 - Local Privilege Escalation | windows/local/[01;31m[K513[m[K41.txt

Student Record System 4.0 - 'cid' SQL Injection | php/webapps/49[01;31m[K513[m[K.txt

sudo 1.8.0 < 1.8.3p1 - 'sudo_debug' glibc FORTIFY_SOURCE Bypass + Privilege Escalation | linux/local/2[01;31m[K513[m[K4.c

Suprema BioStar 2 v2.8.16 - SQL Injection | multiple/webapps/[01;31m[K513[m[K40.txt

Swagger UI 4.1.3 - User Interface (UI) Misrepresentation of Critical Information | json/webapps/[01;31m[K513[m[K79.txt

Symantec Messaging Gateway 10.7.4 - Stored Cross-Site Scripting (XSS) | multiple/webapps/[01;31m[K513[m[K42.txt

Syslog Watcher Pro 2.8.0.812 - 'Date' Cross-Site Scripting | windows/dos/2[01;31m[K513[m[K5.txt

TeamSpeak Client 3.0.18.1 - Remote File Inclusion / Remote Code Execution |
windows/remote/38[01;31m[K513[m[K.txt

Technicolor DT[01;31m[K513[m[K0 2.05.C29GV - Multiple Vulnerabilities
| hardware/webapps/35462.txt

Technicolor TD[01;31m[K513[m[K0.2 - Remote Command Execution
| hardware/webapps/47651.txt

Telindus 1100 Series Router - Administration Password Leak
| hardware/remote/21[01;31m[K513[m[K.c

Tenda N300 F3 12.01.01.48 - Malformed HTTP Request Header Processing
| hardware/remote/[01;31m[K513[m[K17.py

Ultra Shareware Office Control - ActiveX HttpUpload Buffer Overflow (Metasploit) |
windows/remote/16[01;31m[K513[m[K.rb

Unified Remote 3.13.0 - Remote Code Execution (RCE)
| windows/remote/[01;31m[K513[m[K09.py

Universal Media Server 7.1.0 - SSDP Processing XML External Entity Injection |
xml/webapps/4[01;31m[K513[m[K3.txt

VICIdial Manager - Send OS Command Injection (Metasploit)
| linux/remote/29[01;31m[K513[m[K.rb

Vivotek IP Cameras - Multiple Vulnerabilities
| hardware/webapps/2[01;31m[K513[m[K9.txt

VNews 1.2 - Multiple SQL Injections
| php/webapps/27[01;31m[K513[m[K.txt

WebsiteBaker v2.13.3 - Cross-Site Scripting (XSS)
| php/webapps/[01;31m[K513[m[K49.txt

WIMAX SWC-5100W Firmware V(1.11.0.1 :1.9.9.4) - Authenticated RCE
| hardware/remote/[01;31m[K513[m[K11.py

WinArchiver 3.2 - Local Buffer Overflow (SEH)
| windows/local/2[01;31m[K513[m[K1.py

Wondershare Dr Fone 12.9.6 - Privilege Escalation
| windows/local/[01;31m[K513[m[K24.txt

Wondershare Filmora 12.2.9.2233 - Unquoted Service Path
| windows/local/[01;31m[K513[m[K95.txt

WordPress Plugin Accept Signups 0.1 - 'email' Cross-Site Scripting
| php/webapps/3[01;31m[K513[m[K6.txt

WordPress Plugin CP Polls 1.0.8 - Multiple Vulnerabilities
| php/webapps/39[01;31m[K513[m[K.txt

WordPress Plugin Event Registration 5.32 - SQL Injection
| php/webapps/15[01;31m[K513[m[K.txt

WordPress Plugin Mediatricks Viva Thumbs - Multiple Information
Disclosure Vulnerabilities |
php/webapps/3[01;31m[K513[m[K3.txt

WordPress Plugin Photo album - SQL Injection
| php/webapps/[01;31m[K513[m[K5.txt

WordPress Plugin W3 Total Cache - PHP Code Execution (Metasploit)
| php/remote/2[01;31m[K513[m[K7.rb

X2CRM v6.6/6.9 - Reflected Cross-Site Scripting (XSS) (Authenticated)
| php/webapps/[01;31m[K513[m[K46.txt

X2CRM v6.6/6.9 - Stored Cross-Site Scripting (XSS) (Authenticated)
| php/webapps/[01;31m[K513[m[K45.txt

xinkaa Web station 1.0.3 - Directory Traversal
| multiple/remote/2[01;31m[K513[m[K3.txt

XPWeb 3.3.2 - 'url' Remote File Disclosure
| php/webapps/[01;31m[K513[m[K7.txt

ZCBS/ZBBS/ZPBS v4.14k - Reflected Cross-Site Scripting (XSS)
| cgi/webapps/[01;31m[K513[m[K47.txt

-- ----------

-- ----------

Shellcode Title
| Path

-- ----------

Linux/x86 - execve(/bin/sh) Shellcode (25 bytes)
| linux_x86/47[01;31m[K513[m[K.c

Linux/x86 - Reverse (::FFFF:192.168.1.5:4444/TCP) Shell (/bin/sh) +
Null-Free + IPv6 Shellcode (86 bytes) | linux_x86/4[01;31m[K513[m[K9.c

Windows/ARM (Mobile 6.5 TR) - Phone Call Shellcode
| windows/1[01;31m[K513[m[K6.cpp

Windows/x64 - Delete File shellcode / Dynamic PEB method null-free Shellcode |
windows/[01;31m[K513[m[K90.asm

Windows/x86 - PEB 'Kernel32.dll' ImageBase Finder + ASCII Printable Shellcode (49 bytes) |
windows_x86/13[01;31m[K513[m[K.c

Port: 514

Exploit Title
| Path

Achievo 1.4.3 - Cross-Site Request Forgery
| php/webapps/1[01;31m[K514[m[K6.txt

Achievo 1.4.3 - Multiple Authorisation Vulnerabilities
| php/webapps/1[01;31m[K514[m[K5.txt

admidio v4.2.5 - CSV Injection
| php/webapps/[01;31m[K514[m[K02.txt

Adobe Acrobat ActiveX Control 1.3.188 - ActiveX Buffer Overflow
| windows/remote/19[01;31m[K514[m[K.txt

Advanced Host Monitor v12.56 - Unquoted Service Path
| windows/local/[01;31m[K514[m[K12.txt

Affiliate Me Version 5.0.1 - SQL Injection
| php/webapps/[01;31m[K514[m[K68.txt

ALeadSoft Search Engine Builder - Search.HTML Cross-Site Scripting
| java/webapps/30[01;31m[K514[m[K.txt

Aleza Portal 1.6 - Insecure SQL Injection / Cookie Handling
| windows/webapps/1[01;31m[K514[m[K4.txt

Anevia Flamingo XS 3.6.5 - Authenticated Root Remote Code Execution
| hardware/remote/51[01;31m[K514[m[K.txt

Apache Superset 2.0.0 - Authentication Bypass
| multiple/webapps/[01;31m[K514[m[K47.py

appRain 3.0.2 - Blind SQL Injection
| php/webapps/29[01;31m[K514[m[K.txt

Appweb Web Server 3.2.2-1 - Cross-Site Scripting
| multiple/remote/3[01;31m[K514[m[K4.txt

ATutor 2.2.1 - SQL Injection / Remote Code Execution (Metasploit)
| php/remote/39[01;31m[K514[m[K.rb

AudioCoder 0.8.18 - Local Buffer Overflow (SEH)
| windows/local/2[01;31m[K514[m[K1.rb

AvailScript Jobs Portal Script - (Authenticated) Arbitrary File Upload
| php/webapps/6[01;31m[K514[m[K.txt

Avant Browser 11.0 build 26 - Remote Stack Overflow Crash
| windows/dos/3[01;31m[K514[m[K.pl

Beckhoff CX9020 CPU Module - Remote Code Execution
| hardware/webapps/38[01;31m[K514[m[K.py

Best POS Management System v1.0 - Unauthenticated Remote Code Execution
| php/webapps/[01;31m[K514[m[K62.py

Biz Mail Form 2.x - Unauthorized Mail Relay
| cgi/webapps/2[01;31m[K514[m[K7.txt

Bludit CMS v3.14.1 - Stored Cross-Site Scripting (XSS) (Authenticated)
| php/webapps/[01;31m[K514[m[K76.txt

Camaleon CMS v2.7.0 - Server-Side Template Injection (SSTI)
| ruby/webapps/[01;31m[K514[m[K89.txt

Cameleon CMS 2.7.4 - Persistent Stored XSS in Post Title
| ruby/webapps/[01;31m[K514[m[K46.txt

CartWIZ 1.10 - 'Access.asp' Cross-Site Scripting
| asp/webapps/25[01;31m[K514[m[K.txt

cgit < 1.2.1 - 'cgit_clone_objects()' Directory Traversal
| cgi/webapps/4[01;31m[K514[m[K8.txt

ChurchCRM v4.5.4 - Reflected XSS via Image (Authenticated)
| php/webapps/[01;31m[K514[m[K77.txt

CiviCRM 5.59.alpha1 - Stored XSS (Cross-Site Scripting)
| php/webapps/[01;31m[K514[m[K78.txt

Cmaps v8.0 - SQL injection
| php/webapps/[01;31m[K514[m[K22.txt

Codigo Markdown Editor v1.0.1 (Electron) - Remote Code Execution
| multiple/local/[01;31m[K514[m[K32.txt

```
Companymaps v8.0 - Stored Cross Site Scripting (XSS)
| php/webapps/[01;31m[K514[m[K17.txt

D-Link DNS-323 - Multiple Vulnerabilities
| hardware/webapps/2[01;31m[K514[m[K2.txt

dblog - 'dblog.mdb' Remote Database Disclosure
| windows/webapps/10[01;31m[K514[m[K.txt

DESlock+ < 3.2.6 - 'DLMFDISK.sy's Local kernel Ring0 SYSTEM
| windows/local/[01;31m[K514[m[K4.c

DESlock+ < 3.2.6 - 'DLMFENC.sys' Local Kernel Ring0 link list zero
(PoC)                                    |
windows/dos/[01;31m[K514[m[K2.c

DESlock+ < 3.2.6 - 'LIST' Local Kernel Memory Leak
| windows/local/[01;31m[K514[m[K1.c

DESlock+ < 3.2.6 - Local Kernel Ring0 link list zero SYSTEM
| windows/local/[01;31m[K514[m[K3.c

e107 0.7.23 - SQL Injection
| php/webapps/1[01;31m[K514[m[K3.txt

e107 v2.3.2 - Reflected XSS
| php/webapps/[01;31m[K514[m[K49.txt

EasyPHP Webserver 14.1 - Multiple Vulnerabilities (RCE and Path
Traversal)                                  |
php/webapps/[01;31m[K514[m[K30.txt

Eggdrop Server Module Message Handling - Remote Buffer Overflow
| linux/remote/4[01;31m[K514[m[K.c

Elkagroup Image Gallery 1.0 - Arbitrary File Upload
| php/webapps/8[01;31m[K514[m[K.txt

Epson Stylus SX510W Printer Remote Power Off - Denial of Service
| hardware/remote/[01;31m[K514[m[K41.txt

eScan Management Console 14.0.1400.2281 - Cross Site Scripting
| windows/webapps/[01;31m[K514[m[K67.txt

eScan Management Console 14.0.1400.2281 - SQL Injection (Authenticated)
| windows/webapps/[01;31m[K514[m[K66.txt

Faculty Evaluation System 1.0 - Unauthenticated File Upload
| php/webapps/[01;31m[K514[m[K95.py

File Thingie 2.5.7 - Remote Code Execution (RCE)
| php/webapps/[01;31m[K514[m[K36.py
```

```
Filmora 12 version ( Build 1.0.0.7) - Unquoted Service Paths Privilege
Escalation                          |
windows/local/[01;31m[K514[m[K83.txt

FLEX 1080 < 1085 Web 1.6.0 - Denial of Service
| android/dos/[01;31m[K514[m[K38.py

Flexense HTTP Server 10.6.24 - Buffer Overflow (DoS) (Metasploit)
| multiple/remote/[01;31m[K514[m[K93.rb

Fortinet FortiClient 5.2.3 (Windows 10 x64 Creators) - Local Privilege
Escalation                          | windows_x86-
64/local/4[01;31m[K514[m[K9.cpp

Foxit Reader 4.1.1 - Stack Overflow
| windows/dos/15[01;31m[K514[m[K.txt

FS-S3900-24T4S - Privilege Escalation
| hardware/local/[01;31m[K514[m[K14.py

FusionInvoice 2023-1.0 - Stored XSS (Cross-Site Scripting)
| multiple/webapps/[01;31m[K514[m[K80.txt

GetSimple CMS v3.3.16 - Remote Code Execution (RCE)
| php/webapps/[01;31m[K514[m[K75.py

Gin Markdown Editor v0.7.4 (Electron) - Arbitrary Code Execution
| multiple/local/[01;31m[K514[m[K69.txt

GLPI 9.5.7 - Username Enumeration
| php/webapps/[01;31m[K514[m[K18.py

Haihaisoft Universal Player 1.5.8 - '.m3u' / '.pls '/ '.asx' Buffer
Overflow (SEH)                      |
windows/dos/32[01;31m[K514[m[K.py

HotWeb Scripts HotWeb Rentals - 'PageId' SQL Injection
| php/webapps/3[01;31m[K514[m[K3.txt

Hubstaff 1.6.14-61e5e22e - 'wow64log' DLL Search Order Hijacking
| windows/local/[01;31m[K514[m[K61.txt

I-Rater Basic - SQL Injection
| php/webapps/7[01;31m[K514[m[K.txt

IBM Tivoli Access Manager 6.1.1 for E-Business - Directory Traversal
| linux/remote/3[01;31m[K514[m[K8.txt

iGeneric iG Shop 1.x - Multiple SQL Injections
| php/webapps/2[01;31m[K514[m[K9.txt

Invision Power Board (IP.Board) 1.x/2.0.3 - SML Code Script Injection
| php/webapps/2[01;31m[K514[m[K3.txt
```

```
IPtools 0.1.4 - Remote Buffer Overflow
| windows/remote/36[01;31m[K514[m[K.pl

iTech Dating Script 3.40 - SQL Injection
| php/webapps/42[01;31m[K514[m[K.txt

JE CMS 1.0.0 - Authentication Bypass
| php/webapps/1[01;31m[K514[m[K1.txt

Jedox 2020.2.5 - Disclosure of Database Credentials via Improper Access
Controls                          | php/webapps/[01;31m[K514[m[K28.txt

Jedox 2020.2.5 - Remote Code Execution via Configurable Storage Path
| php/webapps/[01;31m[K514[m[K26.txt

Jedox 2020.2.5 - Remote Code Execution via Executable Groovy-Scripts
| php/webapps/[01;31m[K514[m[K27.txt

Jedox 2020.2.5 - Stored Cross-Site Scripting in Log-Module
| php/webapps/[01;31m[K514[m[K25.txt

Jedox 2022.4.2 - Code Execution via RPC Interfaces
| php/webapps/[01;31m[K514[m[K23.txt

Jedox 2022.4.2 - Disclosure of Database Credentials via Connection
Checks                                    |
php/webapps/[01;31m[K514[m[K29.txt

Jedox 2022.4.2 - Remote Code Execution via Directory Traversal
| php/webapps/[01;31m[K514[m[K24.txt

Job Portal 1.0 - File Upload Restriction Bypass
| php/webapps/[01;31m[K514[m[K40.txt

Joomla! Component com_clasifier - 'cat_id' SQL Injection
| php/webapps/[01;31m[K514[m[K6.txt

Joomla! Component com_pccookbook - 'user_id' SQL Injection
| php/webapps/[01;31m[K514[m[K5.txt

Joomla! Component paxxgallery 0.2 - 'gid' Blind SQL Injection
| php/webapps/5[01;31m[K514[m[K.pl

KodExplorer v4.51.03 - Pwned-Admin File-Inclusion - Remote Code
Execution (RCE)                             |
php/webapps/[01;31m[K514[m[K19.txt

LeadPro CRM v1.0 - SQL Injection
| php/webapps/[01;31m[K514[m[K71.txt

LightBlog 9.6 - 'Username' Local File Inclusion
| php/webapps/[01;31m[K514[m[K0.txt
```

```
Linux Kernel - UDP Fragmentation Offset 'UFO' Privilege Escalation
(Metasploit)                                |
linux/local/4[01;31m[K514[m[K7.rb

Linux Kernel 3.10.0-[01;31m[K514[m[K.21.2.el7.x86_64 / 3.10.0-
[01;31m[K514[m[K.26.1.el7.x86_64 (CentOS 7) - SUID Position Independen
| linux/local/42887.c

LiveZilla 3.2.0.2 - 'Track' Module 'server.php' Cross-Site Scripting
| php/webapps/3[01;31m[K514[m[K9.txt

Micro CMS 1.0 b1 - Persistent Cross-Site Scripting
| php/webapps/1[01;31m[K514[m[K7.txt

Microsoft Excel - SxView Record Parsing Heap Memory Corruption
| windows/dos/1[01;31m[K514[m[K8.txt

Microsoft Windows - NTFS Owner/Mandatory Label Privilege Bypass
| windows/dos/43[01;31m[K514[m[K.cs

Microsoft Windows Media Player 11.0.5721.[01;31m[K514[m[K5 - '.avi'
Buffer Overflow                                     |
windows/dos/35553.pl

Microsoft Windows Media Player 11.0.5721.[01;31m[K514[m[K5 - '.mpg'
Buffer Overflow                                     |
windows/dos/11531.pl

MilleGPG5 5.9.2 (Gennaio 2023) - Local Privilege Escalation / Incorrect
Access Control                      |
windows/local/[01;31m[K514[m[K10.txt

MiniNuke 1.8.2b - 'pages.asp' SQL Injection
| asp/webapps/1[01;31m[K514[m[K.pl

MobileTrans  4.0.11 - Weak Service Privilege Escalation
| windows/local/[01;31m[K514[m[K79.txt

Mod_NTLM 0.x - Authorisation Format String
| multiple/dos/22[01;31m[K514[m[K.txt

Mono 1.0.5 - Unicode Character Conversion Multiple Cross-Site Scripting
Vulnerabilities                    | asp/webapps/2[01;31m[K514[m[K8.txt

MotoCMS Version 3.4.3 - Server-Side Template Injection (SSTI)
| multiple/webapps/[01;31m[K514[m[K99.txt

MyBB 1.6 - 'private.php?keywords' SQL Injection
| php/webapps/3[01;31m[K514[m[K1.txt

MyBB 1.6 - 'search.php?keywords' SQL Injection
| php/webapps/3[01;31m[K514[m[K0.txt
```

```
n@board 3.1.9e - 'naboard_pnr.php' Remote File Inclusion
| php/webapps/2[01;31m[K514[m[K.txt

Novell iPrint Client - ActiveX Control ExecuteRequest Buffer Overflow
(Metasploit)                          |
windows/remote/16[01;31m[K514[m[K.rb

Online Clinic Management System 2.2 - Multiple Stored Cross-Site
Scripting (XSS)                           |
php/webapps/[01;31m[K514[m[K39.txt

Online Pizza Ordering System v1.0 - Unauthenticated File Upload
| php/webapps/[01;31m[K514[m[K31.py

Online Security Guards Hiring System 1.0 - Reflected XSS
| php/webapps/[01;31m[K514[m[K94.py

OpenConnect WebConnect 6.4/6.5 - jretest.html Traversal Arbitrary File
Access                                |
windows/remote/2[01;31m[K514[m[K6.txt

OpenEMR v7.0.1 - Authentication credentials brute force
| php/webapps/[01;31m[K514[m[K13.py

Optoma 1080PSTX Firmware C02 - Authentication Bypass
| hardware/remote/[01;31m[K514[m[K44.txt

OrangeHRM 2.6.2 - 'jobVacancy.php' Cross-Site Scripting
| php/webapps/35[01;31m[K514[m[K.txt

PANews 2.0 - PHP Remote Code Execution
| php/webapps/2[01;31m[K514[m[K5.txt

PaperCut NG/MG 22.0.4 - Remote Code Execution (RCE)
| multiple/webapps/[01;31m[K514[m[K52.py

PHP < 5.6.2 - 'Shellshock' Safe Mode / disable_functions Bypass /
Command Injection                       |
php/webapps/3[01;31m[K514[m[K6.txt

PHP Template Store Script 3.0.6 - Cross-Site Scripting
| php/webapps/4[01;31m[K514[m[K3.txt

PHP-Nuke 5.0 - Viewslink SQL Injection
| php/webapps/12[01;31m[K514[m[K.txt

PHP-Nuke Module books SQL - 'cid' SQL Injection
| php/webapps/[01;31m[K514[m[K7.txt

PHPFusion 9.10.30 - Stored Cross-Site Scripting (XSS)
| php/webapps/[01;31m[K514[m[K11.txt
```

PHPJabbers Simple CMS 5.0 - SQL Injection
| php/webapps/[01;31m[K514[m[K16.txt

PHPJabbers Simple CMS V5.0 - Stored Cross-Site Scripting (XSS)
| php/webapps/[01;31m[K514[m[K15.txt

phpMyAdmin 3.x - Swekey Remote Code Injection
| php/webapps/17[01;31m[K514[m[K.php

PHPWCMS 1.2.5 -DEV - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/26[01;31m[K514[m[K.txt

Plex Media Server 1.13.2.5154 - SSDP Processing XML External Entity
Injection |
xml/webapps/4[01;31m[K514[m[K6.txt

Pligg CMS 1.1.3 - 'range' SQL Injection
| php/webapps/3[01;31m[K514[m[K5.txt

pluck v4.7.18 - Stored Cross-Site Scripting (XSS)
| php/webapps/[01;31m[K514[m[K20.txt

PnPSCADA v2.x - Unauthenticated PostgreSQL Injection
| hardware/webapps/[01;31m[K514[m[K48.txt

PodcastGenerator 3.2.9 - Multiple Stored Cross-Site Scripting (XSS)
| php/webapps/[01;31m[K514[m[K54.txt

Prestashop 8.0.4 - CSV injection
| php/webapps/[01;31m[K514[m[K63.txt

projectSend r1605 - Private file download
| php/webapps/[01;31m[K514[m[K00.txt

Pydio Cells 4.1.2 - Cross-Site Scripting (XSS) via File Download
| go/webapps/[01;31m[K514[m[K97.txt

Pydio Cells 4.1.2 - Server-Side Request Forgery
| go/webapps/[01;31m[K514[m[K98.txt

Pydio Cells 4.1.2 - Unauthorised Role Assignments
| go/webapps/[01;31m[K514[m[K96.txt

Quick Classifieds 1.0 - 'style/default.scheme.inc?DOCUMENT_ROOT' Remote
File Inclusion | php/webapps/31[01;31m[K514[m[K.txt

Quicklancer v1.0 - SQL Injection
| php/webapps/[01;31m[K514[m[K74.txt

revive-adserver v5.4.1 - Cross-Site Scripting (XSS)
| php/webapps/[01;31m[K514[m[K01.txt

RockMongo 1.1.7 - Stored Cross-Site Scripting (XSS)
| php/webapps/[01;31m[K514[m[K37.txt

Rukovoditel 3.3.1 - CSV injection
| php/webapps/[01;31m[K514[m[K90.txt

SCM Manager 1.60 - Cross-Site Scripting Stored (Authenticated)
| multiple/webapps/[01;31m[K514[m[K88.py

Screen SFT DAB 600/C - Authentication Bypass Account Creation
| hardware/remote/[01;31m[K514[m[K55.py

Screen SFT DAB 600/C - Authentication Bypass Admin Password Change
| hardware/remote/[01;31m[K514[m[K58.py

Screen SFT DAB 600/C - Authentication Bypass Erase Account
| hardware/remote/[01;31m[K514[m[K57.py

Screen SFT DAB 600/C - Authentication Bypass Password Change
| hardware/remote/[01;31m[K514[m[K56.py

Screen SFT DAB 600/C - Authentication Bypass Reset Board Config
| hardware/remote/[01;31m[K514[m[K59.py

Screen SFT DAB 600/C - Unauthenticated Information Disclosure
(userManager.cgx) |
hardware/remote/[01;31m[K514[m[K60.txt

Scripts Genie Pet Rate Pro - Multiple Vulnerabilities
| php/webapps/24[01;31m[K514[m[K.txt

SCRMS 2023-05-27 1.0 - Multiple SQL Injection
| php/webapps/[01;31m[K514[m[K91.txt

sCssBoard (Multiple Versions) - 'pwnpack' Remote s
| php/webapps/[01;31m[K514[m[K9.rb

sd server 4.0.70 - Directory Traversal
| windows/remote/2[01;31m[K514[m[K4.txt

Seagate Central Storage 2015.0916 - Unauthenticated Remote Command
Execution (Metasploit) |
hardware/remote/[01;31m[K514[m[K87.rb

Serendipity 2.4.0 - File Inclusion RCE
| php/webapps/[01;31m[K514[m[K03.txt

Service Provider Management System v1.0 - SQL Injection
| php/webapps/[01;31m[K514[m[K82.txt

SigPlus Pro 3.74 - ActiveX 'LCDWriteString()' Remote Buffer Overflow
JIT Spray (ASLR + DEP Bypass) |
windows/remote/14[01;31m[K514[m[K.html

```
Single Theater Booking Script - 'newsid' SQL Injection
| php/webapps/41[01;31m[K514[m[K.txt

SitemagicCMS 4.4.3 - Remote Code Execution (RCE)
| php/webapps/[01;31m[K514[m[K64.txt

Smart School v1.0 - SQL Injection
| php/webapps/[01;31m[K514[m[K72.txt

Social Share - 'search' Cross-Site Scripting
| php/webapps/3[01;31m[K514[m[K2.txt

SoftExpert (SE) Suite v2.1.3 - Local File Inclusion
| php/webapps/[01;31m[K514[m[K04.sh

Solaris 10 (Intel) - 'dtprintinfo' Local Privilege Escalation (2)
| solaris/local/49[01;31m[K514[m[K.c

Solaris 2.5.1/2.6/7.0/8 - patchadd Race Condition
| solaris/local/20[01;31m[K514[m[K.pl

Splatt Forum 3.0 - Image Tag HTML Injection
| php/webapps/21[01;31m[K514[m[K.txt

SQL-Ledger 2.6.x/LedgerSMB 1.0 - 'Terminal' Directory Traversal
| cgi/webapps/28[01;31m[K514[m[K.txt

Stackposts Social Marketing Tool v1.0 - SQL Injection
| php/webapps/[01;31m[K514[m[K73.txt

Synology DiskStation Manager - smart.cgi Remote Command Execution
(Metasploit)                              |
hardware/remote/48[01;31m[K514[m[K.rb

TeamCity < 9.0.2 - Disabled Registration Bypass
| multiple/remote/46[01;31m[K514[m[K.js

thrsrossi Millhouse-Project 1.414 - Remote Code Execution
| php/webapps/[01;31m[K514[m[K50.php

TinyWebGallery v2.5 - Remote Code Execution (RCE)
| php/webapps/[01;31m[K514[m[K43.txt

TinyWebGallery v2.5 - Stored Cross-Site Scripting (XSS)
| php/webapps/[01;31m[K514[m[K42.txt

Trend Micro Control Manger 5.5 - 'CmdProcessor.exe' Remote Stack Buffer
Overflow (Metasploit)                     |
windows/remote/18[01;31m[K514[m[K.rb

Trend Micro OfficeScan Client 10.0 - ACL Service LPE
| windows/local/[01;31m[K514[m[K53.txt
```

Tribq CMS 5.2.7 - Cross-Site Request Forgery (Adding/Editing New Administrator Account) | php/webapps/27[01;31m[K514[m[K.txt

Ulicms 2023.1 - create admin user via mass assignment | php/webapps/[01;31m[K514[m[K86.txt

Ulicms-2023.1 sniffing-vicuna - Remote Code Execution (RCE) | php/webapps/[01;31m[K514[m[K34.txt

Ulicms-2023.1 sniffing-vicuna - Stored Cross-Site Scripting (XSS) | php/webapps/[01;31m[K514[m[K35.txt

Ulicms-2023.1-sniffing-vicuna - Privilege escalation | php/webapps/[01;31m[K514[m[K33.py

unilogies/bumsys v1.0.3 beta - Unrestricted File Upload | php/webapps/[01;31m[K514[m[K92.txt

Videos Tube 1.0 - Multiple SQL Injections | php/webapps/33[01;31m[K514[m[K.txt

VLC Media Player/Kodi/PopcornTime 'Red Chimera' < 2.2.5 - Memory Corruption (PoC) | windows/dos/44[01;31m[K514[m[K.py

Vuze Bittorrent Client 5.7.6.0 - SSDP Processing XML External Entity Injection | xml/webapps/4[01;31m[K514[m[K5.txt

WBCE CMS 1.6.1 - Multiple Stored Cross-Site Scripting (XSS) | php/webapps/[01;31m[K514[m[K84.txt

WBiz Desk 1.2 - SQL Injection | php/webapps/[01;31m[K514[m[K51.txt

Webcam Corp Webcam Watchdog 1.0/1.1/3.63 Web Server - Remote Buffer Overflow | windows/remote/23[01;31m[K514[m[K.pl

Webkul Qloapps 1.5.2 - Cross-Site Scripting (XSS) | php/webapps/[01;31m[K514[m[K65.txt

Wedding Slideshow Studio 1.36 - Buffer Overflow | windows/local/4[01;31m[K514[m[K2.py

Wolf CMS 0.8.3.1 - Remote Code Execution (RCE) | php/webapps/[01;31m[K514[m[K21.txt

WordPress Plugin ACF Frontend Display 2.0.5 - Arbitrary File Upload | php/webapps/37[01;31m[K514[m[K.txt

```
WordPress Plugin Backup Migration 1.2.8 - Unauthenticated Database
Backup                                    |
php/webapps/[01;31m[K514[m[K45.txt

WordPress Plugin Slideshow Gallery 1.4.6 - Arbitrary File Upload
| php/webapps/34[01;31m[K514[m[K.txt

WordPress Plugin WP Symposium Pro 2021.10 - 'wps_admin_forum_add_name'
Stored Cross-Site Scripting (XSS)   |
php/webapps/50[01;31m[K514[m[K.txt

WPS Office - 'Wpsio.dll' Stack Buffer Overflow
| windows/dos/2[01;31m[K514[m[K0.txt

WUZHICMS 2.0 - Cross-Site Scripting
| php/webapps/45[01;31m[K514[m[K.txt

Xerox WorkCentre (Multiple Models) - Denial of Service
| hardware/dos/9[01;31m[K514[m[K.py

XOOPS Module myTopics - 'articleId' SQL Injection
| php/webapps/[01;31m[K514[m[K8.txt

Yank Note v3.52.1 (Electron) - Arbitrary Code Execution
| multiple/local/[01;31m[K514[m[K70.txt

Zenphoto 1.6 - Multiple stored XSS
| php/webapps/[01;31m[K514[m[K85.txt

---------------------------------------------------------------------------------------- ----------------
----------

---------------------------------------------------------------------------------------- ----------------
----------
Shellcode Title
|  Path

---------------------------------------------------------------------------------------- ----------------
----------
Linux/ARM - Bind (4444/TCP) Shell (/bin/sh) + IPv6 Shellcode (128
Bytes)                                    | arm/4[01;31m[K514[m[K4.c

Linux/x86 - Reverse (127.0.0.1:4444/TCP) Shell (/bin/sh) + Null-Free
Shellcode (91 bytes)                   | linux_x86/47[01;31m[K514[m[K.c

Windows/x86 - Reverse (/TCP) + Download File + Save + Execute Shellcode
| windows_x86/13[01;31m[K514[m[K.asm

---------------------------------------------------------------------------------------- ----------------
----------
```

Port: 53

Exploit Title
| Path

(Bitcoin / Dogecoin) PHP Cloud Mining Script - Authentication Bypass
| php/webapps/42[01;31m[K53[m[K1.txt

10-Strike Network Inventory Explorer 8.54 - 'Add' Local Buffer Overflow (SEH) |
windows/local/482[01;31m[K53[m[K.py

12Planet Chat Server 2.9 - Cross-Site Scripting
| multiple/remote/242[01;31m[K53[m[K.txt

2[01;31m[K53[m[K2/Gigs 1.2.1 - 'activateuser.php' Local File Inclusion
| php/webapps/4317.txt

2[01;31m[K53[m[K2/Gigs 1.2.2 - Arbitrary Database Backup/Download
| php/webapps/5465.txt

2[01;31m[K53[m[K2/Gigs 1.2.2 Stable - Multiple Vulnerabilities
| php/webapps/7510.txt

2[01;31m[K53[m[K2/Gigs 1.2.2 Stable - Remote Authentication Bypass
| php/webapps/7511.txt

2[01;31m[K53[m[K2/Gigs 1.2.2 Stable - Remote Command Execution
| php/webapps/7512.php

2DayBiz ybiz Network Community Script - SQL Injection / Cross-Site Scripting |
php/webapps/341[01;31m[K53[m[K.txt

3Com OfficeConnect Routers - Remote Denial of Service
| hardware/dos/105[01;31m[K53[m[K.rb

4Images 1.7.1 - Local File Inclusion / Remote Code Execution
| php/webapps/1[01;31m[K53[m[K3.php

68KB 1.0.0rc4 - Remote File Inclusion
| php/webapps/14[01;31m[K53[m[K4.txt

A10 Networks ACOS 2.7.0-P2 (Build [01;31m[K53[m[K) - Buffer Overflow (PoC) |
hardware/dos/32702.txt

Absolute Form Processor XE-V 1.5 - Remote Change Password
| asp/webapps/8[01;31m[K53[m[K0.html

ACC IMoveis 4.0 - SQL Injection
| php/webapps/1[01;31m[K53[m[K38.txt

Accipiter DirectServer 6.0 - Remote File Disclosure
| windows/remote/23[01;31m[K53[m[K3.txt

ACG News 1.0 - 'index.php' Multiple SQL Injections
| php/webapps/30[01;31m[K53[m[K9.txt

Achievo 1.4.5 - Multiple Vulnerabilities (2)
| php/webapps/232[01;31m[K53[m[K.txt

ACollab - 't' SQL Injection
| php/webapps/3[01;31m[K53[m[K05.txt

ACROS Security 0patch 2016.05.19.[01;31m[K53[m[K9 -
'0PatchServicex64.exe' Unquoted Service Path Privilege Escalation |
windows_x86-64/local/39984.txt

ACS Blog 0.8/0.9/1.0/1.1 - 'Name' HTML Injection
| asp/webapps/2[01;31m[K53[m[K13.txt

Active Auction House - 'account.asp?ReturnURL' Cross-Site Scripting
| asp/webapps/2[01;31m[K53[m[K49.txt

Active Auction House - 'default.asp' Multiple SQL Injections
| asp/webapps/2[01;31m[K53[m[K46.txt

Active Auction House - 'ItemInfo.asp' SQL Injection
| asp/webapps/2[01;31m[K53[m[K47.txt

Active Auction House - 'sendpassword.asp' Multiple Cross-Site Scripting
Vulnerabilities | asp/webapps/2[01;31m[K53[m[K51.txt

Active Auction House - 'start.asp?ReturnURL' Cross-Site Scripting
| asp/webapps/2[01;31m[K53[m[K48.txt

Active Auction House - 'WatchThisItem.asp' Cross-Site Scripting
| asp/webapps/2[01;31m[K53[m[K52.txt

Active Calendar 1.2 - '/data/mysqlevents.php?css' Cross-Site Scripting
| php/webapps/296[01;31m[K53[m[K.txt

Active Link Engine - 'default.asp?catid' SQL Injection
| asp/webapps/3[01;31m[K53[m[K4.txt

Active Photo Gallery - 'catid' SQL Injection
| asp/webapps/3[01;31m[K53[m[K6.txt

ActivePerl 5.6.1 - 'perlIIS.dll' Remote Buffer Overflow (2)
| windows/remote/211[01;31m[K53[m[K.c

Acunetix WVS Reporter 10.0 - Denial of Service (PoC)
| windows_x86-64/dos/4[01;31m[K53[m[K11.py

AdMentor - Admin Login SQL Injection
| asp/webapps/29[01;31m[K53[m[K3.html

Admidio 3.3.5 - Cross-Site Request Forgery (Change Permissions)
| php/webapps/4[01;31m[K53[m[K22.txt

Admin News Tools 2.5 - 'fichier' Remote File Disclosure
| php/webapps/91[01;31m[K53[m[K.txt

Adobe Acrobat Reader and Flash Player - 'newclass' Invalid Pointer
| windows/remote/148[01;31m[K53[m[K.py

Adobe Digital Editions 4.5.0 - '.pdf' Critical Memory Corruption
| windows/dos/39[01;31m[K53[m[K3.txt

Adobe Flash AS2 - DisplacementMapFilter.mapBitmap Use-After-Free (1)
| windows/dos/378[01;31m[K53[m[K.txt

Adobe Flash Player - Nellymoser Audio Decoding Buffer Overflow
(Metasploit) |
multiple/remote/37[01;31m[K53[m[K6.rb

Adobe Flash Player 10.2.1[01;31m[K53[m[K.1 - SWF Memory Corruption
(Metasploit) |
windows/remote/17175.rb

Adobe Flash Player < 10.1.[01;31m[K53[m[K.64 - Action Script Type
Confusion (ASLR + DEP Bypass) |
windows/remote/17187.txt

Adobe Flash TextField.text Setter - Use-After-Free
| windows/dos/390[01;31m[K53[m[K.txt

Adobe Photoshop CS4 Extended 11.0 - '.ASL' File Handling Remote Buffer
Overflow (PoC) | windows/dos/127[01;31m[K53[m[K.c

Adobe RoboHelp 9 - DOM Cross-Site Scripting
| cgi/webapps/176[01;31m[K53[m[K.txt

Advanced Comment System 1.0 - SQL Injection
| php/webapps/458[01;31m[K53[m[K.txt

Advanced File Management 1.4 - 'users.php' Cross-Site Scripting
| php/webapps/36[01;31m[K53[m[K9.txt

Advanced Poll 2.0.2 - 'common.inc.php' Remote File Inclusion
| php/webapps/282[01;31m[K53[m[K.txt

```
Advanced Poll 2.0.2/2.0.3 - 'popup.php' Cross-Site Scripting
| php/webapps/26[01;31m[K53[m[K9.txt

Advantech EKI-6340 - Command Injection
| cgi/webapps/3[01;31m[K53[m[K57.txt

Affiliate Directory - 'cat_id' SQL Injection
| php/webapps/[01;31m[K53[m[K63.txt

AIDA64 Engineer 6.20.[01;31m[K53[m[K00 - 'Report File' filename Buffer
Overflow (SEH)                                    |
windows/local/48281.py

AIM Triton 1.0.4 - CSeq Buffer Overflow (Metasploit)
| windows/remote/163[01;31m[K53[m[K.rb

Aimeos Laravel ecommerce platform 2021.10 LTS - 'sort' SQL injection
| php/webapps/50[01;31m[K53[m[K8.txt

AIMP2 Audio Converter 2.[01;31m[K53[m[K build 330 - Playlist '.pls'
Unicode Buffer Overflow                           |
windows/local/10280.py

AIMP2 Audio Converter 2.[01;31m[K53[m[Kb330 - '.pls' / '.m3u' Unicode
Crash (PoC)                                         | windows/dos/9561.py

AirLive (Multiple Products) - OS Command Injection
| hardware/webapps/37[01;31m[K53[m[K2.txt

AirTies Air[01;31m[K53[m[K41 Modem 1.0.0.12 - Cross-Site Request
Forgery                                                 |
hardware/webapps/462[01;31m[K53[m[K.html

Airties AIR[01;31m[K53[m[K42 1.0.0.18 - Cross-Site Scripting
| hardware/webapps/45525.txt

All In One 1.4 Control Panel - 'cp_polls_results.php' SQL Injection
| php/webapps/32[01;31m[K53[m[K7.txt

All In One Control Panel 1.4.1 - 'cp_menu_data_file.php' SQL Injection
| php/webapps/3[01;31m[K53[m[K07.py

allomani 2007 - 'cat' SQL Injection
| php/webapps/9[01;31m[K53[m[K2.txt

Alreader 2.5 .fb2 - Based Stack Overflow (SEH) (ASLR + DEP Bypass)
| windows/local/38[01;31m[K53[m[K2.py

Alstrasoft e-Friends 4.96 - Multiple Vulnerabilities
| php/webapps/1[01;31m[K53[m[K35.txt

Alstrasoft EPay Pro 2.0 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/2[01;31m[K53[m[K28.txt
```

```
Alstrasoft EPay Pro 2.0 - Remote File Inclusion
| php/webapps/2[01;31m[K53[m[K27.txt

Alt-N MDaemon 12.5.6/13.0.3 - Email Body HTML/JS Injection
| windows/webapps/24[01;31m[K53[m[K4.txt

Alt-N MDaemon webmail 20.0.0 - 'Contact name' Stored Cross Site
Scripting (XSS)                              |
windows/webapps/49[01;31m[K53[m[K6.txt

Alt-N MDaemon webmail 20.0.0 - 'file name' Stored Cross Site Scripting
(XSS)                                  |
windows/webapps/49[01;31m[K53[m[K7.txt

Alt-N MDaemon WorldClient 13.0.3 - Multiple Vulnerabilities
| windows/webapps/24[01;31m[K53[m[K5.txt

Altova DatabaseSpy 2011 - Project File Handling Buffer Overflow (PoC)
| windows/dos/1[01;31m[K53[m[K01.pl

AMD Fuel Service - 'Fuel.service' Unquote Service Path
| windows/local/49[01;31m[K53[m[K5.txt

amfPHP 1.2 - '/browser/details?class' Cross-Site Scripting
| php/webapps/316[01;31m[K53[m[K.txt

AN HTTPD - 'CMDIS.dll' Remote Buffer Overflow (PoC)
| windows/dos/2[01;31m[K53[m[K64.txt

AN HTTPD 1.42 - Arbitrary Log Content Injection
| windows/remote/2[01;31m[K53[m[K65.txt

Android - 'zygote->init;' Chain from USB Privilege Escalation
| android/local/4[01;31m[K53[m[K79.txt

Android WAPPushManager - SQL Injection
| android/dos/3[01;31m[K53[m[K82.txt

Andy's PHP Projects Man Page Lookup Script - Information Disclosure
| php/webapps/23[01;31m[K53[m[K6.txt

Angular-Base64-Upload Library 0.1.21 - Unauthenticated Remote Code
Execution (RCE)                            |
multiple/webapps/522[01;31m[K53[m[K.py

AnnonceScriptHP 2.0 - 'voirannonce.php?no' SQL Injection
| php/webapps/292[01;31m[K53[m[K.txt

Anuko Time Tracker 1.19.23.[01;31m[K53[m[K11 - No rate Limit on
Password Reset functionality                                 |
php/webapps/49173.txt
```

Anuko Time Tracker 1.19.23.[01;31m[K53[m[K11 - Password Reset leading to Account Takeover |
php/webapps/49174.txt

Anuko Time Tracker 1.19.23.[01;31m[K53[m[K25 - CSV/Formula Injection
| php/webapps/49027.txt

Any Sound Recorder 2.93 - Denial of Service (PoC)
| windows_x86/dos/4[01;31m[K53[m[K56.py

AnyDVD 6.7.1.0 - Denial of Service
| windows_x86/dos/1[01;31m[K53[m[K06.pl

Apache 1.1 / NCSA HTTPd 1.5.2 / Netscape Server 1.12/1.1/2.0 - a nph-test-cgi |
multiple/dos/19[01;31m[K53[m[K6.txt

Apache 2.0 mod_jk2 2.0.2 (Windows x86) - Remote Buffer Overflow
| windows_x86/remote/[01;31m[K53[m[K30.c

Apache 2.2 (Windows) - Local Denial of Service
| windows/dos/1[01;31m[K53[m[K19.pl

Apache Portals Pluto 3.0.0 - Remote Code Execution
| windows/webapps/4[01;31m[K53[m[K96.txt

Apache Roller 5.0.3 - XML External Entity Injection (File Disclosure)
| linux/webapps/4[01;31m[K53[m[K41.py

Apache Struts 2 - Namespace Redirect OGNL Injection (Metasploit)
| multiple/remote/4[01;31m[K53[m[K67.rb

Apache Tomcat - 'WebDAV' Remote File Disclosure
| multiple/remote/4[01;31m[K53[m[K0.pl

Apache Tomcat 3/4 - 'DefaultServlet' File Disclosure
| unix/remote/218[01;31m[K53[m[K.txt

Apache Tomcat 3/4 - JSP Engine Denial of Service
| linux/dos/21[01;31m[K53[m[K4.jsp

Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (|
windows/webapps/429[01;31m[K53[m[K.txt

Apache Tomcat Connector jk2-2.0.2 mod_jk2 - Remote Overflow
| linux/remote/[01;31m[K53[m[K86.txt

Apple Installer Package 2.1.5 - Filename Format String
| osx/dos/29[01;31m[K53[m[K2.txt

Apple iOS - '.pdf' Local Privilege Escalation 'Jailbreak'
| ios/local/14[01;31m[K53[m[K8.txt

```
Apple Mac OSX (Mavericks) - 'IOBluetoothHCIUserClient' Privilege
Escalation                                  |
osx/dos/351[01;31m[K53[m[K.c

Apple Mac OSX - Java applet Remote Deserialization Remote (2)
| osx/remote/87[01;31m[K53[m[K.txt

Apple Mac OSX 10.4.x - Help Viewer '.help' Filename Format String
| osx/dos/295[01;31m[K53[m[K.txt

Apple macOS 10.13.4 - Denial of Service (PoC)
| macos/dos/4[01;31m[K53[m[K91.py

Apple OS X/iOS Kernel - IOSurface Use-After-Free
| osx/local/406[01;31m[K53[m[K.txt

Apple Safari - User-Assisted Applescript Exec Attack (Metasploit)
| osx/remote/38[01;31m[K53[m[K5.rb

Apple Safari 4.0.4 ([01;31m[K53[m[K1.21.10) - Stack Overflow / Denial
of Service                                          |
windows/dos/11601.pl

Apple Safari 4.0.5 ([01;31m[K53[m[K1.22.7) - Denial of Service
| windows/dos/12408.pl

Apple WebKit 10.0.2 - 'Frame::setDocument' Universal Cross-Site
Scripting                                   |
multiple/webapps/414[01;31m[K53[m[K.html

Apport 2.19 (Ubuntu 15.04) - Local Privilege Escalation
| linux/local/383[01;31m[K53[m[K.txt

ArGoSoft FTP Server 1.4.3.5 - Remote Buffer Overflow (PoC)
| windows/dos/1[01;31m[K53[m[K1.pl

Argus Surveillance DVR 4.0.0.0 - Privilege Escalation
| windows_x86/local/4[01;31m[K53[m[K12.c

Arris VAP2500 - Authentication Bypass
| hardware/webapps/3[01;31m[K53[m[K72.rb

Article Friendly - SQL Injection
| php/webapps/11[01;31m[K53[m[K0.txt

Artmedic CMS 3.4 - 'index.php' Local File Inclusion
| php/webapps/4[01;31m[K53[m[K8.txt

Ask.com/AskJeeves Toolbar Toolbar 4.0.2.[01;31m[K53[m[K - ActiveX
Remote Buffer Overflow                                  |
windows/remote/4452.html
```

```
ASP Simple Blog 3.0 - Arbitrary File Upload
| multiple/webapps/107[01;31m[K53[m[K.txt

ASP-DEV XM Forum RC3 - IMG Tag Script Injection
| asp/webapps/2[01;31m[K53[m[K24.txt

Astium VoIP PBX 2.1 build 2[01;31m[K53[m[K99 - Multiple
Vulnerabilities/Remote Command Execution                          |
php/webapps/23831.py

Astium VoIP PBX 2.1 build 2[01;31m[K53[m[K99 - Remote Crash (PoC)
| linux/dos/23830.py

ASUS Net4Switch - 'ipswcom.dll' ActiveX Stack Buffer Overflow
(Metasploit)                                      |
windows/remote/18[01;31m[K53[m[K8.rb

ASUSWRT RT-AC[01;31m[K53[m[K (3.0.0.4.380.6038) - Cross-Site Scripting
| hardware/webapps/41571.txt

ASUSWRT RT-AC[01;31m[K53[m[K (3.0.0.4.380.6038) - Remote Code Execution
| hardware/webapps/41573.txt

ASUSWRT RT-AC[01;31m[K53[m[K (3.0.0.4.380.6038) - Session Stealing
| hardware/webapps/41572.txt

Atheros Coex Service Application 8.0.0.255 - 'ZAtheros Bt&Wlan Coex
Agent' Unquoted Service Path           |
windows/local/490[01;31m[K53[m[K.txt

AtHocGov IWSAlerts - ActiveX Control Buffer Overflow (Metasploit)
| windows/remote/16[01;31m[K53[m[K4.rb

ATutor 1.6.1-pl1 - 'import.php' Remote File Inclusion
| php/webapps/61[01;31m[K53[m[K.txt

Audio Workstation - '.pls' Local Buffer Overflow (SEH)
| windows/local/103[01;31m[K53[m[K.pl

AuraCMS 2.x - '/user.php' Security Code Bypass / Arbitrary Add
Administrator                                     |
php/webapps/[01;31m[K53[m[K19.pl

Auto CMS 1.6 - 'autocms.php' Cross-Site Scripting
| php/webapps/34[01;31m[K53[m[K3.txt

Auto CMS 1.8 - Remote Code Execution
| php/webapps/1[01;31m[K53[m[K69.php

AutoIndex PHP Script 2.2.1 - 'index.php' Cross-Site Scripting
| php/webapps/30[01;31m[K53[m[K1.txt
```

```
AutoIndex PHP Script 2.2.2/2.2.3 - 'index.php' Denial of Service
| php/dos/307[01;31m[K53[m[K.txt

Avast aswSnx.sys Kernel Driver 11.1.22[01;31m[K53[m[K - Memory
Corruption Privilege Escalation                          |
windows/dos/42182.cpp

Avast! - Authenticode Parsing Memory Corruption
| windows/dos/39[01;31m[K53[m[K0.txt

Avast! Internet Security 5.0 - 'aswFW.sys' Kernel Driver IOCTL Memory
Pool Corruption                      |
windows/dos/14[01;31m[K53[m[K3.txt

AVG Internet Security 2015.0.[01;31m[K53[m[K15 - Arbitrary Write
Privilege Escalation                                     |
windows/local/35993.c

AVG Internet Security 9.0.851 - Local Denial of Service
| windows/dos/1[01;31m[K53[m[K84.c

AwindInc SNMP Service - Command Injection (Metasploit)
| linux/remote/473[01;31m[K53[m[K.rb

AWStats 5.7 < 6.2 - Multiple Remote s
| cgi/webapps/8[01;31m[K53[m[K.c

Ayman Akt IRCIT 0.3.1 - Invite Message Remote Buffer Overflow
| linux/dos/21[01;31m[K53[m[K7.c

Azaronline Design - SQL Injection
| php/webapps/1[01;31m[K53[m[K91.txt

Azerbaijan Development Group AzDGDatingPlatinum 1.1.0 - 'view.php?id'
Cross-Site Scripting                |
php/webapps/2[01;31m[K53[m[K73.txt

Azerbaijan Development Group AzDGDatingPlatinum 1.1.0 - 'view.php?id'
SQL Injection                       |
php/webapps/2[01;31m[K53[m[K74.txt

B2B Classic Trading Script - 'offers.php' SQL Injection
| php/webapps/12[01;31m[K53[m[K2.txt

BaoFeng Storm - 'mps.dll' ActiveX OnBeforeVideoDownload Buffer Overflow
(Metasploit)                        |
windows/remote/165[01;31m[K53[m[K.rb

Barracuda Spam Firewall 3.3.03.0[01;31m[K53[m[K - Remote Code Execution
(1)                                                      |
hardware/remote/2136.txt
```

Barracuda Spam Firewall 3.3.03.0[01;31m[K53[m[K - Remote Code Execution (2) |
hardware/remote/2145.txt

Barracuda SSL VPN 680 - 'returnTo' Open Redirection
| hardware/remote/38[01;31m[K53[m[K6.txt

basebuilder 2.0.1 - 'main.inc.php' Remote File Inclusion
| php/webapps/6[01;31m[K53[m[K3.txt

Basic Analysis and Security Engine (BASE) 1.4.5 - 'base_stat_time.php?base_path' Remote File Inclusion |
php/webapps/367[01;31m[K53[m[K.txt

Basilix Webmail 0.9.7 - Incorrect File Permissions
| php/webapps/20[01;31m[K53[m[K8.txt

Batavi 1.0 - Multiple Local File Inclusion / Cross-Site Scripting Vulnerabilities |
php/webapps/3[01;31m[K53[m[K62.txt

Battlefield 2/2142 - Packet Null Pointer Dereference Remote Denial of Service |
multiple/dos/3[01;31m[K53[m[K69.txt

Bayanno Hospital Management System 4.0 - Cross-Site Scripting
| php/webapps/4[01;31m[K53[m[K75.txt

bcoos 1.0.13 - 'click.php' SQL Injection
| php/webapps/32[01;31m[K53[m[K6.txt

bcoos 1.0.13 - 'common.php' Remote File Inclusion
| php/webapps/32[01;31m[K53[m[K2.txt

Berlios GPSD - Format String (Metasploit)
| linux/remote/168[01;31m[K53[m[K.rb

BES-CMS 0.4/0.5 - 'index.inc.php' File Inclusion
| php/webapps/234[01;31m[K53[m[K.txt

BetaParticle blog 2.0/3.0 - 'upload.asp' Arbitrary File Upload
| asp/webapps/252[01;31m[K53[m[K.txt

Betsy 4.0 - 'page' Local File Inclusion
| php/webapps/3[01;31m[K53[m[K09.txt

big.asp - SQL Injection
| php/webapps/12[01;31m[K53[m[K3.txt

BigACE 2.7.3 - Cross-Site Request Forgery (Change Admin Password)
| php/webapps/1[01;31m[K53[m[K20.py

```
BitchX 1.0 - Remote 'Send_CTCP()' Memory Corruption
| linux/remote/223[01;31m[K53[m[K.c

Bitweaver 1.x - '/blogs/list_blogs.php?sort_mode' SQL Injection
| php/webapps/289[01;31m[K53[m[K.txt

BlackBoard Academic Suite 6/7 -
'/bin/common/announcement.pl?data__announcements___pk1_pk2__subject'
Cross | cgi/webapps/31[01;31m[K53[m[K8.txt

BlackBoard Academic Suite 6/7 -
'/webapps/BlackBoard/execute/viewCatalog?searchText' Cross-Site
Scripting  | cgi/webapps/31[01;31m[K53[m[K7.txt

BlastChat Client 3.3 - Cross-Site Scripting
| php/webapps/34[01;31m[K53[m[K1.txt

BLOG 1.55B - 'image_upload.php' Arbitrary File Upload
| php/webapps/7[01;31m[K53[m[K7.txt

Blog Master Pro 1.0 - CSV Injection
| php/webapps/44[01;31m[K53[m[K5.txt

Blog PixelMotion - 'categorie' SQL Injection
| php/webapps/[01;31m[K53[m[K82.txt

Blog PixelMotion - 'modif_config.php' Arbitrary File Upload
| php/webapps/[01;31m[K53[m[K81.txt

Blog PixelMotion - 'sauvBase.php' Arbitrary Database Backup
| php/webapps/[01;31m[K53[m[K80.txt

Blogator-script 0.95 - 'id_art' SQL Injection
| php/webapps/[01;31m[K53[m[K68.txt

Blogator-script 0.95 - 'incl_page' Remote File Inclusion
| php/webapps/[01;31m[K53[m[K65.txt

Blogator-script 0.95 - Change User Password
| php/webapps/[01;31m[K53[m[K70.txt

BlogBird Platform - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/1[01;31m[K53[m[K32.txt

BlogEngine.NET 3.3.6 - Directory Traversal / Remote Code Execution
| aspx/webapps/463[01;31m[K53[m[K.cs

BlogMe PHP 1.1 - 'comments.php' SQL Injection
| php/webapps/5[01;31m[K53[m[K3.txt

BlogWrite 0.91 - Remote File Disclosure / SQL Injection
| php/webapps/80[01;31m[K53[m[K.pl
```

Bloodshed Dev-C++ 4.9.9.2 - Multiple EXE Loading Arbitrary Code Executions |
windows/remote/34[01;31m[K53[m[K2.c

BloofoxCMS 0.3.5 - Information Disclosure
| php/webapps/1[01;31m[K53[m[K26.txt

BloofoxCMS Registration Plugin - SQL Injection
| php/webapps/1[01;31m[K53[m[K28.txt

BLUE COM Router [01;31m[K53[m[K60/52018 - Password Reset
| hardware/webapps/31088.py

Blueberry Express 5.9.0.3678 - Local Buffer Overflow (SEH)
| windows/local/37[01;31m[K53[m[K5.txt

BlueSoleil 1.4 - Object Push Service BlueTooth Arbitrary File Upload / Directory Traversal |
windows/remote/2[01;31m[K53[m[K25.txt

Bluethrust Clan Scripts v4 R17 - Multiple Vulnerabilities
| php/webapps/39[01;31m[K53[m[K4.html

Boite de News 4.0.1 - 'index.php' Remote File Inclusion
| php/webapps/21[01;31m[K53[m[K.txt

BolinOS 4.6.1 - Local File Inclusion / Cross-Site Scripting
| php/webapps/[01;31m[K53[m[K09.txt

Bomba Haber 2.0 - 'haberoku.php' SQL Injection
| php/webapps/31[01;31m[K53[m[K1.pl

Booking Centre 2.01 - 'HotelID' SQL Injection
| php/webapps/72[01;31m[K53[m[K.txt

BOOTP Turbo 2.0.0.12[01;31m[K53[m[K - 'bootpt.exe' Unquoted Service Path |
windows/local/49851.txt

Borland Interbase - 'Create-Request' Remote Buffer Overflow (Metasploit) |
windows/remote/164[01;31m[K53[m[K.rb

Borland/Inprise Interbase 4.0/5.0/6.0 - Backdoor Password
| multiple/remote/20[01;31m[K53[m[K7.txt

BoutikOne - 'search.php' Multiple SQL Injections
| php/webapps/354[01;31m[K53[m[K.txt

BPConferenceReporting Web Reporting - Authentication Bypass
| asp/webapps/155[01;31m[K53[m[K.txt

Broadcom PIPA C211 - Sensitive Information Disclosure
| hardware/webapps/333[01;31m[K53[m[K.txt

Brother HL-[01;31m[K53[m[K70DW - series Authentication Bypass printer flooder |
hardware/dos/173[01;31m[K53[m[K.pl

BrowserCRM 5.100.1 - 'clients.php' Cross-Site Scripting
| php/webapps/364[01;31m[K53[m[K.txt

BSA Radar 1.6.7234.24750 - Cross-Site Request Forgery (Change Password)
| hardware/webapps/486[01;31m[K53[m[K.txt

BSI Advance Hotel Booking System 1.0 - SQL Injection
| php/webapps/15[01;31m[K53[m[K1.txt

Buffy 1.3 - Directory Traversal
| windows/remote/1[01;31m[K53[m[K68.php

BugTracker.NET 3.4.4 - Multiple Vulnerabilities
| asp/webapps/156[01;31m[K53[m[K.txt

BulletProof FTP Client 2.45 - Remote Buffer Overflow
| windows/remote/2[01;31m[K53[m[K0.py

Cain & Abel 2.7.3 - 'dagc.dll' DLL Loading Arbitrary Code Execution
| windows/remote/3[01;31m[K53[m[K18.c

Caldera OpenServer 5.0.x - XSCO Color Database File Heap Overflow
| unix/dos/21[01;31m[K53[m[K1.txt

Cartweaver 2.16.11 - 'Results.cfm' SQL Injection
| cfm/webapps/278[01;31m[K53[m[K.txt

Cayin Content Management Server 11.0 - Remote Command Injection (root)
| multiple/webapps/485[01;31m[K53[m[K.txt

CCBILL CGI - 'ccbillx.c' 'whereami.cgi' Remote Code Execution
| cgi/webapps/[01;31m[K53[m[K.c

CCH Wolters Kluwer PFX Engagement 7.1 - Local Privilege Escalation
| windows/local/3[01;31m[K53[m[K95.txt

CDNetworks Nefficient Download - 'NeffyLauncher.dll' Code Execution
| windows/remote/[01;31m[K53[m[K97.txt

CentOS Web Panel 0.9.8.793 (Free) / 0.9.8.7[01;31m[K53[m[K (Pro) - Cross-Site Scripting |
linux/webapps/46669.txt

CentOS Web Panel 0.9.8.793 (Free) / v0.9.8.7[01;31m[K53[m[K (Pro) / 0.9.8.807 (Pro) - Domain Field (Add DNS Zone) Cross |
linux/webapps/46784.txt

```
Cerberus Helpdesk 2.7 - 'Clients.php' Cross-Site Scripting
| php/webapps/271[01;31m[K53[m[K.txt

CGIScript.net csNews 1.0 - Double URL Encoding Unauthorized
Administrative Access                              |
cgi/webapps/21[01;31m[K53[m[K2.txt

CGIScript.net csNews 1.0 - Header File Type Restriction Bypass
| cgi/webapps/21[01;31m[K53[m[K3.txt

Chamilo LMS 1.11.8 - 'firstname' Cross-Site Scripting
| php/webapps/45[01;31m[K53[m[K6.txt

Chamilo LMS 1.11.8 - Cross-Site Scripting
| php/webapps/45[01;31m[K53[m[K5.txt

ChartDirector 4.1 - 'viewsource.php' File Disclosure
| php/webapps/[01;31m[K53[m[K99.txt

Chasys Media Player 1.1 - '.mid' Local Buffer Overflow
| windows/dos/11[01;31m[K53[m[K7.pl

Chatness 2.5 - 'Message Form' HTML Injection
| php/webapps/2[01;31m[K53[m[K15.html

Chicomas 2.0.4 - Database Backup / File Disclosure / Cross-Site
Scripting                                          |
php/webapps/7[01;31m[K53[m[K2.txt

Chilkat XML - ActiveX Arbitrary File Creation/Execution
| windows/remote/6[01;31m[K53[m[K7.html

ChilkatHttp ActiveX 2.3 - Arbitrary Files Overwrite
| windows/remote/[01;31m[K53[m[K38.html

Chipmunk Blog - 'cat.php' Cross-Site Scripting
| php/webapps/319[01;31m[K53[m[K.txt

Chrome 35.0.1916.1[01;31m[K53[m[K - Sandbox Escape / Command Execution
| windows/local/44269.txt

Chrome V8 JIT - 'NodeProperties::InferReceiverMaps' Type Confusion
| multiple/dos/44[01;31m[K53[m[K0.js

CirCarLife SCADA 4.3.0 - Credential Disclosure
| hardware/webapps/4[01;31m[K53[m[K84.py

Cisco AS[01;31m[K53[m[K50 - Universal Gateway Portscan Denial of
Service                                                |
hardware/dos/21971.txt

Cisco IOS 12.0.2 - Syslog Crash
| hardware/dos/19[01;31m[K53[m[K1.txt
```

```
Cisco Umbrella Roaming Client 2.0.168 - Local Privilege Escalation
| windows_x86-64/local/4[01;31m[K53[m[K39.c

Cisco Wireless Controller 3.6.10E - Cross-Site Request Forgery
| hardware/webapps/471[01;31m[K53[m[K.txt

CityPost Simple PHP Upload - 'Simple-upload-[01;31m[K53[m[K.php' Cross-
Site Scripting                                  |
php/webapps/25464.txt

CiviCRM 3.3.3 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K53[m[K27.txt

CJ Ultra Plus 1.0.4 - Cookie SQL Injection
| php/webapps/6[01;31m[K53[m[K6.pl

CKEditor 4.0.1 - Multiple Vulnerabilities
| php/webapps/24[01;31m[K53[m[K0.txt

Claroline E-Learning 1.5/1.6 - 'exercises_details.php?exo_id' SQL
Injection                                       |
php/webapps/255[01;31m[K53[m[K.txt

Claroline E-Learning 1.6 - Remote Hash SQL Injection (2)
| php/webapps/10[01;31m[K53[m[K.pl

ClickCart 6.0 - Authentication Bypass
| php/webapps/79[01;31m[K53[m[K.txt

ClientExec 3.0 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                                 |
php/webapps/300[01;31m[K53[m[K.txt

Clinic Management System 1.0 - Authentication Bypass
| php/webapps/48[01;31m[K53[m[K8.txt

Clipbucket 2.6 - 'channels.php?time' SQL Injection
| php/webapps/36[01;31m[K53[m[K2.txt

Clipbucket 2.6 - 'videos.php?time' SQL Injection
| php/webapps/36[01;31m[K53[m[K1.txt

Clipbucket 2.6 - 'view_item.php?type' Cross-Site Scripting
| php/webapps/36[01;31m[K53[m[K0.txt

Clone2Go Video to iPod Converter 2.5.0 - Denial of Service (PoC)
| windows_x86/dos/4[01;31m[K53[m[K97.py

Cobalt 0.1 - Multiple SQL Injections
| asp/webapps/[01;31m[K53[m[K73.txt
```

Cobalt RaQ 2.0/3.0 / qpopper 2.52/2.[01;31m[K53[m[K - 'EUIDL' Format String Input |
linux/local/19955.c

Code::Blocks - Denial of Service
| multiple/dos/38[01;31m[K53[m[K8.py

Cold BBS - Remote Database Disclosure
| asp/webapps/73[01;31m[K53[m[K.txt

ColdFusion 9-10 - Credential Disclosure
| multiple/webapps/2[01;31m[K53[m[K05.py

Collabtive 0.65 - SQL Injection
| php/webapps/1[01;31m[K53[m[K81.txt

Comdev News Publisher 4.1.2 - SQL Injection
| php/webapps/[01;31m[K53[m[K62.txt

Comersus Cart 4.0/5.0 - 'Comersus_Search_Item.asp' Cross-Site Scripting
| asp/webapps/2[01;31m[K53[m[K90.txt

Comersus Open Technologies Comersus Cart 6.0.41 - Multiple SQL Injections |
asp/webapps/259[01;31m[K53[m[K.txt

Command School Student Management System - '/sw/health_allergies.php?id' SQL Injection |
php/webapps/389[01;31m[K53[m[K.txt

Composr 10.0.36 - Remote Code Execution
| php/webapps/497[01;31m[K53[m[K.txt

Compro Technology IP Camera - ' index_MJpeg.cgi' Stream Disclosure
| hardware/webapps/502[01;31m[K53[m[K.txt

CompuCMS - Multiple SQL Injections / Cross-Site Scripting Vulnerabilities |
php/webapps/34[01;31m[K53[m[K6.txt

Computer Associates InoculateIT 4.[01;31m[K53[m[K - Microsoft Exchange Agent |
windows/local/20401.txt

Comrie Software Pay Roll Time Sheet & Punch Card - Authentication Bypass |
asp/webapps/1[01;31m[K53[m[K96.txt

COMTREND ADSL Router CT-[01;31m[K53[m[K67 C01_R12 - Remote Code Execution |
hardware/remote/16275.txt

COMTREND ADSL Router CT-[01;31m[K53[m[K67 C01_R12 / CT-5624 C01_R03 - DNS Change | cgi/webapps/40372.sh

Comtrend AR-[01;31m[K53[m[K87un router - Persistent XSS (Authenticated) | hardware/webapps/48908.py

COMTREND CT-[01;31m[K53[m[K6 / HG-[01;31m[K53[m[K6 Routers - Multiple Remote Vulnerabilities | hardware/remote/32681.txt

COMTREND CT-[01;31m[K53[m[K61T Router - 'Password.cgi' Cross-Site Request Forgery (Admin Password Manipulation) | hardware/remote/39154.txt

Comtrend-AR-[01;31m[K53[m[K10 - Restricted Shell Escape | linux/local/47149.txt

Conext ComBox 865-1058 - Denial of Service | hardware/dos/41[01;31m[K53[m[K7.py

Configuration Tool 1.6.[01;31m[K53[m[K - 'OpLclSrv' Unquoted Service Path | windows/local/49624.txt

Content Injector 1.[01;31m[K53[m[K - 'index.php' SQL Injection | php/webapps/4706.txt

CoolPlayer 2.19 - '.Skin' Local Buffer Overflow | windows/local/7[01;31m[K53[m[K6.cpp

Corda Highwire - 'Highwire.ashx' Full Path Disclosure | asp/webapps/386[01;31m[K53[m[K.txt

Core FTP 2.0 build 6[01;31m[K53[m[K - 'PBSZ' Denial of Service (PoC) | windows/dos/46[01;31m[K53[m[K2.py

Core FTP Server 1.2 build [01;31m[K53[m[K5 (32-bi)t - Crash (PoC) | windows/dos/33495.py

Core FTP Server FTP / SFTP Server v2 Build 674 - 'MDTM' Directory Traversal | windows/dos/46[01;31m[K53[m[K4.txt

Core FTP Server FTP / SFTP Server v2 Build 674 - 'SIZE' Directory Traversal | windows/dos/46[01;31m[K53[m[K5.txt

cPanel WebHost Manager (WHM) - '/webmail/x3/mail/clientconf.html?acct' Cross-Site Scripting | php/webapps/381[01;31m[K53[m[K.txt

```
CPG Dragonfly 9.0.2.0 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/2[01;31m[K53[m[K16.txt

Cplinks 1.03 - Authentication Bypass / SQL Injection / Cross-Site
Scripting                                  |
php/webapps/5[01;31m[K53[m[K8.txt

Crea8Social 1.3 - Persistent Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K67.txt

Creative Software AutoUpdate Engine - ActiveX Control Buffer Overflow
(Metasploit)                             |
windows/remote/16[01;31m[K53[m[K9.rb

Croogo 1.2.1 - Multiple Cross-Site Request Forgery Vulnerabilities
| php/webapps/113[01;31m[K53[m[K.txt

CrossFire 1.8.0 - 'oldsocketmode' Remote Buffer Overflow (PoC)
| windows/dos/1[01;31m[K53[m[K5.c

Crystal Player 1.98 - '.mls' Buffer Overflow
| windows/dos/34[01;31m[K53[m[K0.py

Crystal Shard http-protection 0.2.0 - IP Spoofing Bypass
| multiple/webapps/48[01;31m[K53[m[K3.py

CubeCart 2.0.x - 'index.php' Multiple Full Path Disclosures
| php/webapps/2[01;31m[K53[m[K55.txt

CubeCart 2.0.x - 'tellafriend.php?product' Full Path Disclosure
| php/webapps/2[01;31m[K53[m[K56.txt

CubeCart 2.0.x - 'view_cart.php?add' Full Path Disclosure
| php/webapps/2[01;31m[K53[m[K57.txt

CubeCart 2.0.x - 'view_product.php?product' Full Path Disclosure
| php/webapps/2[01;31m[K53[m[K58.txt

CyberGhost 6.0.4.2205 - Local Privilege Escalation
| windows/local/41[01;31m[K53[m[K8.cs

Cybrotech CyBroHttpServer 1.0.3 - Cross-Site Scripting
| windows_x86-64/webapps/4[01;31m[K53[m[K09.txt

Cybrotech CyBroHttpServer 1.0.3 - Directory Traversal
| windows_x86-64/webapps/4[01;31m[K53[m[K03.txt

Cyrus IMAPD 2.3.2 - 'pop3d' Remote Buffer Overflow (2)
| multiple/remote/20[01;31m[K53[m[K.rb

D-Link Central WiFiManager Software Controller 1.03 - Multiple
Vulnerabilities                            |
php/webapps/45[01;31m[K53[m[K3.txt
```

D-Link DIR-300 - Cross-Site Request Forgery (Change Admin Account Settings) |
hardware/webapps/157[01;31m[K53[m[K.html

D-Link DIR-600 / DIR-300 (Rev B) - Multiple Vulnerabilities
| hardware/webapps/244[01;31m[K53[m[K.txt

D-Link Dir-600M N150 - Cross-Site Scripting
| hardware/webapps/4[01;31m[K53[m[K43.txt

D-Link DIR-615 - Denial of Service (PoC)
| hardware/dos/4[01;31m[K53[m[K17.txt

D-Link DIR-Series Routers - '/model/__show_info.php' Local File Disclosure |
hardware/webapps/388[01;31m[K53[m[K.sh

Dacio's Image Gallery 1.6 - Directory Traversal / Authentication Bypass / Arbitrary File Upload | php/webapps/86[01;31m[K53[m[K.txt

Daily Habit Tracker 1.0 - SQL Injection
| php/webapps/519[01;31m[K53[m[K.md

Dale Mooney Calendar Events - 'Viewevent.php' SQL Injection
| php/webapps/30[01;31m[K53[m[K3.txt

DamiCMS 6.0.0 - Cross-Site Request Forgery (Change Admin Password)
| php/webapps/4[01;31m[K53[m[K14.txt

DansGuardian Webmin Module 0.x - 'edit.cgi' Directory Traversal
| cgi/webapps/23[01;31m[K53[m[K5.txt

DaqFactory 5.85 build 18[01;31m[K53[m[K - Stack Overflow
| windows/dos/17841.txt

Dark Hart Portal - 'login.php' Remote File Inclusion
| php/webapps/125[01;31m[K53[m[K.txt

Data Dynamics ActiveBar (Actbar3.ocx 3.2) - Multiple Insecure Methods
| windows/remote/[01;31m[K53[m[K95.html

DATAC RealWin SCADA Server 1.06 - Remote Buffer Overflow
| windows/remote/1[01;31m[K53[m[K37.py

David Bagley xlock 4.16 - User Supplied Format String (1)
| unix/local/201[01;31m[K53[m[K.c

DaZPHP 0.1 - 'prefixdir' Local File Inclusion
| php/webapps/[01;31m[K53[m[K47.txt

DBHcms 1.1.4 - 'dbhcms_pid' SQL Injection
| php/webapps/1[01;31m[K53[m[K09.txt

DBHcms 1.1.4 - 'dbhcms_user/SearchString' SQL Injection
| php/webapps/1[01;31m[K53[m[K21.txt

DBImageGallery 1.2.2 - 'donsimg_base_path' Remote File Inclusion
| php/webapps/33[01;31m[K53[m[K.txt

DCP-Portal 6.11 - SQL Injection
| php/webapps/48[01;31m[K53[m[K.php

Debian 2.1 - HTTPd
| linux/remote/192[01;31m[K53[m[K.txt

DeluxeBB 1.07 - Remote Create Admin
| php/webapps/19[01;31m[K53[m[K.pl

Destar 0.2.2-5 - Arbitrary Add Admin
| php/webapps/[01;31m[K53[m[K05.py

Destiny Media Player 1.61 - '.rdl' Local Buffer Overflow
| windows/local/8[01;31m[K53[m[K5.pl

Device42 WAN Emulator 2.3 - Ping Command Injection (Metasploit)
| cgi/webapps/3[01;31m[K53[m[K84.rb

Device42 WAN Emulator 2.3 - Traceroute Command Injection (Metasploit)
| cgi/webapps/3[01;31m[K53[m[K83.rb

DGNews 2.1 - SQL Injection
| php/webapps/158[01;31m[K53[m[K.txt

Diferior CMS 8.03 - Multiple Cross-Site Request Forgery Vulnerabilities
| php/webapps/143[01;31m[K53[m[K.html

Digger Solutions NewsLetter Open Source - SQL Injection
| asp/webapps/1[01;31m[K53[m[K98.txt

Digital Eye CMS 0.1.1b - 'module.php' Remote File Inclusion
| php/webapps/3[01;31m[K53[m[K3.txt

DirectTopics 2 - 'topic.php' SQL Injection
| php/webapps/256[01;31m[K53[m[K.txt

Discuz! 2.0/3.0 - Cross-Site Scripting
| php/webapps/236[01;31m[K53[m[K.txt

Disk Pulse Enterprise 9.9.16 - 'Import Command' Local Buffer Overflow
| windows/local/42[01;31m[K53[m[K6.py

Disk Savvy Enterprise 9.9.14 - 'Import Command' Local Buffer Overflow
| windows/local/42[01;31m[K53[m[K8.py

DivX Player 6.7.0 - '.srt' File Buffer Overflow (PoC)
| windows/dos/54[01;31m[K53[m[K.pl

```
DivX Player 6.x - '.dps' Remote Buffer Overflow
| windows/remote/3[01;31m[K53[m[K99.pl

DLink DIR 819 A1 - Denial of Service
| hardware/dos/510[01;31m[K53[m[K.txt

DLink DIR-601 - Credential Disclosure
| hardware/webapps/4[01;31m[K53[m[K06.txt

dnGuestbook 2.0 - SQL Injection
| php/webapps/16[01;31m[K53[m[K.txt

Dokeos 1.8.4 - Arbitrary File Upload
| php/webapps/47[01;31m[K53[m[K.txt

Dokeos 1.8.6 2 - 'style' Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K47.txt

Dolphin 7.0.4 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K53[m[K32.txt

Dolphin 7.0.x - 'viewFriends.php' Multiple Cross-Site Scripting
Vulnerabilities                              |
php/webapps/368[01;31m[K53[m[K.txt

doop CMS 1.3.7 - Local File Inclusion
| php/webapps/4[01;31m[K53[m[K6.txt

DotBr 0.1 - 'System.php3' Remote Command Execution
| php/webapps/222[01;31m[K53[m[K.txt

dotclear 2.25.3 - Remote Code Execution (RCE) (Authenticated)
| php/webapps/513[01;31m[K53[m[K.txt

douran portal 3.9.7.55 - Multiple Vulnerabilities
| asp/webapps/1[01;31m[K53[m[K82.txt

Dragoon 0.1 - 'lng' Local File Inclusion
| php/webapps/[01;31m[K53[m[K69.txt

Dragoon 0.1 - 'root' Remote File Inclusion
| php/webapps/[01;31m[K53[m[K93.txt

Drake CMS 0.4.11 - Blind SQL Injection
| php/webapps/[01;31m[K53[m[K91.php

Dreamcost HostAdmin 3.1 - 'index.php' Cross-Site Scripting
| php/webapps/324[01;31m[K53[m[K.txt

Drupal Module CAPTCHA - Security Bypass
| php/webapps/3[01;31m[K53[m[K35.html
```

Drupal Module Cumulus 5.x-1.1/6.x-1.4 - 'tagcloud' Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K97.txt

Drupal Module Drag & Drop Gallery 6.x-1.5 - 'upload.php' Arbitrary File
Upload | php/webapps/374[01;31m[K53[m[K.php

DVD Photo Slideshow Professional 8.07 - Buffer Overflow (SEH)
| windows/local/4[01;31m[K53[m[K46.py

dwebpro 6.8.26 - Directory Traversal / File Disclosure
| windows/remote/8[01;31m[K53[m[K7.txt

DZCP (deV!L_z Clanportal) 1.5.4 - Local File Inclusion
| php/webapps/1[01;31m[K53[m[K23.txt

e107 0.7.23 - Multiple SQL Injections
| php/webapps/346[01;31m[K53[m[K.txt

e107 Plugin My_Gallery 2.3 - Arbitrary File Download
| php/webapps/[01;31m[K53[m[K08.txt

e107 website system 0.6 - 'usersettings.php?avmsg' Cross-Site Scripting
| php/webapps/241[01;31m[K53[m[K.txt

Easy File Management Web Server 5.3 - Remote Stack Buffer Overflow
| windows/remote/334[01;31m[K53[m[K.py

Easy File Sharing FTP Server 3.5 - Remote Stack Buffer Overflow
| windows/remote/33[01;31m[K53[m[K8.py

Easy PhotoResQ 1.0 - Denial Of Service (PoC)
| windows_x86/dos/4[01;31m[K53[m[K00.py

EasyFTP Server 1.7.0.2 - CWD Remote Buffer Overflow
| windows/remote/11[01;31m[K53[m[K9.py

Easynet Forum Host - 'forum.php' SQL Injection
| php/webapps/[01;31m[K53[m[K72.txt

Easynet4u Forum Host - 'topic.php' SQL Injection
| php/webapps/337[01;31m[K53[m[K.txt

EasyNews 40tr - SQL Injection / Cross-Site Scripting / Local File
Inclusion |
php/webapps/[01;31m[K53[m[K33.py

EB Design Pty Ltd - 'EBCRYPT.dll 2.0' Multiple Remote Vulnerabilities
| windows/remote/44[01;31m[K53[m[K.html

EFS Easy Chat Server 3.1 - Password Disclosure
| windows/webapps/421[01;31m[K53[m[K.py

EgavilanMedia User Registration & Login System with Admin Panel 1.0 - Stored Cross Site Scripting | multiple/webapps/491[01;31m[K53[m[K.txt

EggBlog 4.0 - SQL Injection | php/webapps/[01;31m[K53[m[K36.pl

Elecard AVC_HD/MPEG Player 5.7 - Local Buffer Overflow | windows/local/162[01;31m[K53[m[K.py

Elecard MPEG Player - '.m3u' Local Stack Overflow | windows/local/78[01;31m[K53[m[K.pl

elFinder PHP Connector < 2.1.48 - 'exiftran' Command Injection (Metasploit) | php/remote/46[01;31m[K53[m[K9.rb

elFinder Web file manager Version - 2.1.[01;31m[K53[m[K Remote Command Execution | php/webapps/51864.txt

Elipse E3 - HTTP Denial of Service | windows/dos/3[01;31m[K53[m[K79.go

elvin bts 1.2.0 - Multiple Vulnerabilities | php/webapps/89[01;31m[K53[m[K.txt

Emacs - movemail Privilege Escalation (Metasploit) | unix/local/459[01;31m[K53[m[K.rb

EMC Celerra NAS Appliance - Unauthorized Access to Root NFS Export | hardware/remote/14[01;31m[K53[m[K6.txt

Emefa Guestbook 3.0 - Remote Database Disclosure | asp/webapps/7[01;31m[K53[m[K4.txt

EncapsCMS 0.3.6 - 'common_foot.php' Remote File Inclusion | php/webapps/29[01;31m[K53[m[K9.txt

EncFS 1.6.0 - Flawed CBC/CFB Cryptography Implementation | linux/local/34[01;31m[K53[m[K7.txt

eNdonesia - 'cid' SQL Injection | php/webapps/375[01;31m[K53[m[K.txt

Energine CMS - SQL Injection | php/webapps/1[01;31m[K53[m[K27.txt

Engineers Online Portal 1.0 - 'id' SQL Injection | php/webapps/504[01;31m[K53[m[K.txt

Entertainment Directory 1.1 - SQL Injection | php/webapps/[01;31m[K53[m[K71.txt

```
Envato Clone Script - SQL Injection
| php/webapps/415[01;31m[K53[m[K.txt

EO Video 1.36 - Local Heap Overflow Denial of Service / (PoC)
| windows/dos/62[01;31m[K53[m[K.py

EPay Enterprise 4.13 - 'cid' SQL Injection
| php/webapps/123[01;31m[K53[m[K.txt

Escortservice 1.0 - 'custid' SQL Injection
| php/webapps/3[01;31m[K53[m[K15.txt

Eshopbuilde CMS - SQL Injection
| asp/webapps/102[01;31m[K53[m[K.txt

ETicket 1.5.5 - 'Open.php' Multiple Cross-Site Scripting
Vulnerabilities                                      |
php/webapps/302[01;31m[K53[m[K.txt

Eve-ng 5.0.1-13 - Stored Cross-Site Scripting (XSS)
| php/webapps/511[01;31m[K53[m[K.txt

EveryAuction 1.[01;31m[K53[m[K - Auction.pl Cross-Site Scripting
| cgi/webapps/26786.txt

Exim 4.84-3 - Local Privilege Escalation
| linux/local/39[01;31m[K53[m[K5.sh

EXoops - Multiple Input Validation Vulnerabilities
| php/webapps/2[01;31m[K53[m[K00.txt

Expinion.net Member Management System 2.1 - 'error.asp?err' Cross-Site
Scripting                              |
asp/webapps/238[01;31m[K53[m[K.txt

Explorer32++ v1.3.5.[01;31m[K53[m[K1 - Buffer overflow
| windows/local/51077.txt

eXtremail 1.x/2.1 - Remote Format String (2)
| linux/remote/209[01;31m[K53[m[K.c

eXtremail 2.1.1 - 'LOGIN' Remote Stack Overflow
| linux/remote/4[01;31m[K53[m[K3.c

eXtremail 2.1.1 - 'memmove()' Remote Denial of Service
| linux/dos/4[01;31m[K53[m[K2.pl

eXtremail 2.1.1 - PLAIN Authentication Remote Stack Overflow
| linux/remote/4[01;31m[K53[m[K4.c

eXtremail 2.1.1 - Remote Heap Overflow (PoC)
| linux/dos/4[01;31m[K53[m[K5.pl
```

```
eXtropia bbs_forum.cgi 1.0 - Arbitrary Command Execution
| cgi/remote/20[01;31m[K53[m[K3.txt

eXV2 Module eblog 1.2 - 'blog_id' SQL Injection
| php/webapps/52[01;31m[K53[m[K.txt

EyouCMS 1.4.6 - Persistent Cross-Site Scripting
| php/webapps/48[01;31m[K53[m[K0.txt

EZContents 2.0.3 - 'event_list.php?GLOBALS[admin_home]' Remote File
Inclusion                                 |
php/webapps/284[01;31m[K53[m[K.txt

EZDatabase 2.1.2 - 'index.php?p' Local File Inclusion
| php/webapps/268[01;31m[K53[m[K.txt

Fantastic News 2.1.2 - 'script_path' Remote Code Execution
| php/webapps/15[01;31m[K53[m[K.pl

Farsinews 2.5 - Directory Traversal Arbitrary 'users.db' Access
| php/webapps/1[01;31m[K53[m[K8.pl

FaScript FaPhoto 1.0 - 'show.php' SQL Injection
| php/webapps/[01;31m[K53[m[K34.txt

FastStone 4in1 Browser 1.2 - Web Server Directory Traversal
| windows/remote/2[01;31m[K53[m[K19.txt

FathFTP 1.8 - 'FileExists Method' ActiveX Buffer Overflow (SEH)
| windows/remote/145[01;31m[K53[m[K.html

FathFTP 1.8 - 'RasIsConnected Method' ActiveX Buffer Overflow (SEH)
| windows/remote/14[01;31m[K53[m[K9.html

FD Script 1.3.x - 'FName' Information Disclosure
| php/webapps/29[01;31m[K53[m[K0.txt

Fez 1.3/2.0 RC1 - 'list.php' SQL Injection
| php/webapps/6[01;31m[K53[m[K5.txt

FiberHome LM[01;31m[K53[m[KQ1 - Multiple Vulnerabilities
| hardware/webapps/43460.py

File Transfer 1.2 - Request File Directory Traversal
| windows/remote/31[01;31m[K53[m[K6.txt

File(1) 4.13 - Command File_PrintF Integer Underflow
| linux/remote/297[01;31m[K53[m[K.c

FileBox File Hosting & Sharing Script 1.5 - SQL Injection
| php/webapps/177[01;31m[K53[m[K.txt
```

FipsCMS 2.1 - 'print.asp' SQL Injection
| asp/webapps/55[01;31m[K53[m[K.txt

Firebook - 'index.html' Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K12.txt

Flash Slideshow Maker Professional 5.20 - Buffer Overflow (SEH)
| windows_x86/local/4[01;31m[K53[m[K55.py

FLDS 1.2a - 'redir.php' SQL Injection
| php/webapps/74[01;31m[K53[m[K.txt

Flipper Poll 1.1.0 - 'poll.php?root_path' Remote File Inclusion
| php/webapps/32[01;31m[K53[m[K.txt

FLIR Thermal Traffic Cameras 1.01-0bb5b27 - Information Disclosure
| hardware/webapps/45[01;31m[K53[m[K9.py

FLIR Thermal Traffic Cameras 1.01-0bb5b27 - RTSP Stream Disclosure
| hardware/webapps/45[01;31m[K53[m[K7.txt

Flux Player 3.1.0 iOS - Multiple Vulnerabilities
| ios/webapps/269[01;31m[K53[m[K.txt

FoT Video scripti 1.1b - 'oyun' SQL Injection
| asp/webapps/64[01;31m[K53[m[K.txt

Foxit Reader 4.1.1 - Local Stack Buffer Overflow
| windows/local/15[01;31m[K53[m[K2.py

Free Monthly Websites 2.0 - Admin Password Change
| php/webapps/249[01;31m[K53[m[K.txt

free QBoard 1.1 - 'delete.php?qb_path' Remote File Inclusion
| php/webapps/281[01;31m[K53[m[K.txt

FreeBSD 3.3 - 'angband' Local Buffer Overflow
| freebsd/local/196[01;31m[K53[m[K.c

Freefloat FTP Server 1.0 - 'MKD' Remote Buffer Overflow
| windows/remote/17[01;31m[K53[m[K9.rb

Fritz!Box Webcm - Command Injection (Metasploit)
| hardware/remote/327[01;31m[K53[m[K.rb

FrontPage 97/98 - Server Image Mapper Buffer Overflow
| windows/dos/198[01;31m[K53[m[K.txt

FS Groupon Clone 1.0 - 'id' SQL Injection
| php/webapps/432[01;31m[K53[m[K.txt

```
FsPro Labs Event Log Explorer v4.6.1.2115 - XML External Entity
Injection                                   |
windows/webapps/4[01;31m[K53[m[K19.txt

FTPShell Client 6.[01;31m[K53[m[K - 'Session name' Local Buffer
Overflow                                                  |
windows/dos/41629.py

FTPShell Client 6.[01;31m[K53[m[K - Remote Buffer Overflow
| windows/remote/41511.py

FUJI XEROX DocuCentre-V 3065 Printer - Remote Command Execution
| hardware/remote/4[01;31m[K53[m[K32.py

Fundraising Script 1.0 - SQLi
| php/webapps/517[01;31m[K53[m[K.TXT

FUSE fusermount Tool - Race Condition
| linux/dos/349[01;31m[K53[m[K.txt

Fuzzylime CMS 3.01 - 'poll' Remote Code Execution
| php/webapps/60[01;31m[K53[m[K.php

Gaming Directory 1.0 - 'cat_id' SQL Injection
| php/webapps/[01;31m[K53[m[K74.txt

Ganesha Digital Library 4.0 - Multiple Vulnerabilities
| php/webapps/189[01;31m[K53[m[K.txt

Genepi 1.6 - 'genepi.php' Remote File Inclusion
| php/webapps/2[01;31m[K53[m[K9.txt

GeoGebra Graphing Calculator 6.0.631.0 - Denial Of Service (PoC)
| windows/local/496[01;31m[K53[m[K.py

GeoHttpServer - Remote Denial of Service
| windows/dos/12[01;31m[K53[m[K1.pl

Getsimple CMS 2.03 - 'upload-ajax.php' Arbitrary File Upload
| php/webapps/3[01;31m[K53[m[K[01;31m[K53[m[K.txt

Geutebrueck GCore 1.3.8.42/1.4.2.37 - Remote Code Execution
(Metasploit)                                  |
windows/remote/411[01;31m[K53[m[K.rb

Ghostscript - Failed Restore Command Execution (Metasploit)
| linux/local/4[01;31m[K53[m[K69.rb

GhostScripter Amazon Shop 5.0 - 'search.php' SQL Injection
| php/webapps/266[01;31m[K53[m[K.txt

GitLab 13.10.2 - Remote Code Execution (RCE) (Unauthenticated)
| ruby/webapps/50[01;31m[K53[m[K2.txt
```

```
glFusion 1.1.x/1.2.1 - 'users.php' SQL Injection
| php/webapps/3[01;31m[K53[m[K91.txt

glFusion 1.2.2 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/24[01;31m[K53[m[K6.txt

GLPI 0.83.9 - 'Unserialize()' Remote Code Execution
| php/webapps/26[01;31m[K53[m[K0.txt

GNU C Library 2.x (libc6) - Dynamic Linker LD_AUDIT Arbitrary DSO Load
Privilege Escalation                |
linux/local/1[01;31m[K53[m[K04.txt

GNU gdbserver 9.2 - Remote Command Execution (RCE)
| linux/remote/50[01;31m[K53[m[K9.py

Gollos 2.8 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K53[m[K49.txt

GOM Player 2.1.21.4846 - '.wav' Buffer Overflow
| windows/dos/11[01;31m[K53[m[K6.pl

GOM Player 2.2.[01;31m[K53[m[K.5169 - '.reg' Local Buffer Overflow
(SEH)                                                |
windows/local/30154.pl

GOM Player 2.3.90.[01;31m[K53[m[K60 - Buffer Overflow (PoC)
| windows/local/51724.py

GOM Player 2.3.90.[01;31m[K53[m[K60 - Remote Code Execution (RCE)
| windows/remote/51719.py

GOMPlayer 2.2.[01;31m[K53[m[K.5169 - '.wav' Crash (PoC)
| windows/dos/28080.py

Google Chrome 0.2.149.27 - Denial of Service
| windows/dos/63[01;31m[K53[m[K.txt

Google Chrome 1.0.154.[01;31m[K53[m[K - Null Pointer Remote Crash
| windows/dos/8573.html

Google Chrome 73.0.3683.39 / Chromium 74.0.3712.0 - 'ReadableStream'
Internal Object Leak Type Confusion   |
multiple/dos/466[01;31m[K53[m[K.html

Google Earth 5.1.3[01;31m[K53[m[K5.3218 - 'quserex.dll' DLL Hijacking
| windows/local/14790.c

gpEasy 1.5RC3 - Remote File Inclusion
| php/webapps/10[01;31m[K53[m[K7.txt
```

Gracenote CDDBControl - ActiveX Control 'ViewProfile' Method Heap Buffer Overflow (PoC) | windows/dos/33[01;31m[K53[m[K3.html

Grandstream Budge Tone 101/102 VOIP Phone - Denial of Service | hardware/dos/11[01;31m[K53[m[K.pl

Grandstream Budge Tone-200 IP Phone - Digest domain Denial of Service | hardware/dos/3[01;31m[K53[m[K5.pl

Grandstream GXV3275 < 1.0.3.30 - Multiple Vulnerabilities | hardware/webapps/37[01;31m[K53[m[K1.txt

GrayCMS 1.1 - 'error.php' Remote File Inclusion | php/webapps/25[01;31m[K53[m[K8.txt

Graylog Collector 0.4.2 - Unquoted Service Path Privilege Escalation | windows/local/40[01;31m[K53[m[K8.txt

Green Dam - URL Processing Buffer Overflow (Metasploit) | windows/remote/16[01;31m[K53[m[K6.rb

Gregarius 0.6.1 - Multiple SQL Injections / Cross-Site Scripting | php/webapps/36[01;31m[K53[m[K8.txt

GRR Système de Gestion et de Réservations de Ressources 3.0.0-RC1 - Arbitrary File Upload | php/webapps/401[01;31m[K53[m[K.txt

gSOAP 2.8 - Directory Traversal | php/webapps/476[01;31m[K53[m[K.txt

Hand-Crafted Software FreeProxy 3.5/3.6 - FreeWeb CreateFile Function Denial of Service | windows/dos/23[01;31m[K53[m[K4.txt

Hand-Crafted Software FreeProxy 3.5/3.6 - FreeWeb Directory Traversal | windows/remote/23[01;31m[K53[m[K2.txt

HD Soft Windows FTP Server 1.5/1.6 - 'Username' Format String | windows/remote/23[01;31m[K53[m[K1.c

Helix Server 11.0.1 (Windows 2000 SP4) - Remote Heap Overflow | windows/remote/3[01;31m[K53[m[K1.py

Hikvision DVR - RTSP Request Remote Code Execution (Metasploit) | linux/remote/3[01;31m[K53[m[K56.rb

HIS-Webshop - 'his-webshop.pl t' Remote File Disclosure | cgi/webapps/[01;31m[K53[m[K04.txt

HiSecOS 04.0.01 - Privilege Escalation | hardware/webapps/51[01;31m[K53[m[K7.sh

```
HLDS WebMod 0.48 - 'rconpass' Remote Heap Overflow
| windows/remote/5[01;31m[K53[m[K6.php

HLDS WebMod 0.48 - Multiple Remote Vulnerabilities
| multiple/remote/5[01;31m[K53[m[K4.txt

Home FTP Server 1.11.1.149 - 'RETR'/'DELE'/'RMD' Directory Traversal
| windows/remote/1[01;31m[K53[m[K57.php

Home FTP Server 1.11.1.149 - (Authenticated) Directory Traversal
| windows/remote/1[01;31m[K53[m[K49.txt

HongCMS 3.0.0 - (Authenticated) SQL Injection
| php/webapps/449[01;31m[K53[m[K.txt

Horde Application Framework 3.2.1 - Forward Slash Insufficient
Filtering Cross-Site Scripting              |
php/webapps/323[01;31m[K53[m[K.txt

Hosting Controller 6.1 - 'resellerresources.asp?jresourceid' SQL
Injection                                   |
asp/webapps/257[01;31m[K53[m[K.txt

HP Data Protector Media Operations 6.11 - HTTP Server Remote Integer
Overflow Denial of Service            |
windows/dos/1[01;31m[K53[m[K07.py

HP Network Node Manager (NMM) i 9.10 - '/nnm/mibdiscover?node' Cross-
Site Scripting                          |
jsp/webapps/363[01;31m[K53[m[K.txt

HP OpenView Network Node Manager (OV NNM) - 'Toolbar.exe' CGI Cookie
Handling Buffer Overflow (Metasploit) |
windows/remote/17[01;31m[K53[m[K7.rb

HP OpenView Network Node Manager (OV NNM) 7.5.1 - 'OVAS.exe' Overflow
(SEH)                                   |
windows/remote/[01;31m[K53[m[K42.py

HP OpenView Network Node Manager (OV NNM) 7.[01;31m[K53[m[K -
'ovalarm.exe' CGI Remote Buffer Overflow                  |
windows/remote/10394.py

HP OpenView Network Node Manager (OV NNM) 7.[01;31m[K53[m[K -
'OvJavaLocale' Buffer Overflow                            |
windows/webapps/14547.txt

HP OpenView Network Node Manager (OV NNM) 7.[01;31m[K53[m[K -
'ovwebsnmpsrv.exe' Local Buffer Overflow (SEH)            |
windows/local/14256.txt
```

HP OpenView Network Node Manager (OV NNM) 7.[01;31m[K53[m[K - Invalid DB Error Code | windows/dos/10176.txt

HP OpenView Network Node Manager (OV NNM) 7.[01;31m[K53[m[K - Multiple Vulnerabilities | windows/dos/[01;31m[K53[m[K96.txt

HP OpenView Network Node Manager (OV NNM) 7.[01;31m[K53[m[K/7.51 - 'OVAS.exe' Stack Buffer Overflow (Metasploit) | windows/remote/16774.rb

HP OpenView Network Node Manager 7.[01;31m[K53[m[K - Multiple Vulnerabilities | multiple/remote/5430.txt

HP-UX 10.20 newgrp - Local Privilege Escalation | hp-ux/local/19[01;31m[K53[m[K5.pl

HPE iLO 4 < 2.[01;31m[K53[m[K - Add New Administrator User | multiple/remote/44005.py

HRSALE The Ultimate HRM 1.0.2 - 'award_id' SQL Injection | php/webapps/44[01;31m[K53[m[K7.txt

HRSALE The Ultimate HRM 1.0.2 - (Authenticated) Cross-Site Scripting | php/webapps/44[01;31m[K53[m[K8.txt

HRSALE The Ultimate HRM 1.0.2 - CSV Injection | php/webapps/44[01;31m[K53[m[K6.txt

HRSALE The Ultimate HRM 1.0.2 - Local File Inclusion | php/webapps/44[01;31m[K53[m[K9.txt

HSPell 1.1 - 'cilla.cgi' Remote Command Execution | cgi/webapps/77[01;31m[K53[m[K.pl

HTML5 Video Player 1.2.5 - Denial of Service (PoC) | windows_x86/dos/4[01;31m[K53[m[K76.py

httpdx 1.4 - GET Buffer Overflow | windows/remote/100[01;31m[K53[m[K.txt

Huawei E[01;31m[K53[m[K30 21.210.09.00.158 - Cross-Site Request Forgery (Send SMS) | hardware/webapps/46092.py

Huawei E[01;31m[K53[m[K31 MiFi Mobile Hotspot 21.344.11.00.414 - Multiple Vulnerabilities | hardware/webapps/32161.txt

Huawei HG[01;31m[K53[m[K2n - Command Injection (Metasploit) | hardware/remote/41895.rb

Huawei Router HG[01;31m[K53[m[K2 - Arbitrary Command Execution
| hardware/webapps/43414.py

Huawei Router HG[01;31m[K53[m[K2e - Command Execution
| hardware/webapps/45991.py

Hybrid Networks Cable Broadband Access System 1.0 - Remote
Configuration |
hardware/remote/19[01;31m[K53[m[K8.txt

I-Gallery - Folder Argument Directory Traversal
| asp/webapps/258[01;31m[K53[m[K.txt

Iatek IntranetApp 2.3 - 'ad_click.asp?banner_id' SQL Injection
| asp/webapps/2[01;31m[K53[m[K18.txt

IBM AIX 4.3 - '/usr/lib/lpd/digest' Local Buffer Overflow
| aix/local/204[01;31m[K53[m[K.c

IBM AIX 4.3.2 - 'ftpd' Remote Buffer Overflow
| aix/remote/19[01;31m[K53[m[K2.pl

IBM HTTP Server 1.3 - AfpaCache/WebSphereNet.Data Denial of Service
| multiple/dos/20[01;31m[K53[m[K1.txt

IBM Identity Governance and Intelligence 5.2.3.2 / 5.2.4 - SQL
Injection |
php/webapps/4[01;31m[K53[m[K92.txt

IBM iSeries AS400 LDAP Server - Remote Information Disclosure
| unix/remote/2[01;31m[K53[m[K35.txt

IBM Lotus Domino Server 6.5.1 Web Service - Remote Denial of Service
| unix/dos/2[01;31m[K53[m[K[01;31m[K53[m[K.txt

IBM Lotus Sametime - '/stconf.nsf/WebMessage?messageString' Cross-Site
Scripting |
multiple/remote/3[01;31m[K53[m[K64.txt

IBM Lotus Sametime - stconf.nsf Cross-Site Scripting
| multiple/remote/3[01;31m[K53[m[K66.txt

IBM Lotus Sametime Server 8.0 - 'stcenter.nsf' Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K74.txt

IBM Personal Communications I-Series Access Workstation 5.9 - Profile
(Metasploit) |
windows/remote/18[01;31m[K53[m[K9.rb

IBM RICOH Infoprint 1[01;31m[K53[m[K2 Printer - Persistent Cross-Site
Scripting |
hardware/webapps/47850.txt

IBM Websphere/Net.Commerce 3 - CGI-BIN Macro Denial of Service
| cgi/dos/207[01;31m[K53[m[K.txt

iCash 7.6.5 - Denial of Service (PoC)
| windows/dos/4[01;31m[K53[m[K88.py

Icy Phoenix 1.3.0.[01;31m[K53[m[Ka - HTTP Referer Persistent Cross-Site Scripting | php/webapps/16199.txt

iDevAffiliate - 'idevads.php' SQL Injection
| php/webapps/391[01;31m[K53[m[K.txt

IDM 6.20 - Local Buffer Overflow
| windows/local/36[01;31m[K53[m[K3.py

IKE - Aggressive Mode Shared Secret Hash Leakage
| hardware/remote/22[01;31m[K53[m[K2.txt

Image Gallery with Access Database - 'dispimage.asp?id' SQL Injection
| asp/webapps/290[01;31m[K53[m[K.txt

ImageVue 1.7 - 'dir2.php?path' Cross-Site Scripting
| php/webapps/313[01;31m[K53[m[K.txt

IMAP4rev1 10.190 - Authentication Stack Overflow
| linux/remote/2[01;31m[K53[m[K.pl

ImpressPages CMS 1.0x - 'admin.php' Multiple SQL Injections
| php/webapps/340[01;31m[K53[m[K.txt

ImTOO MPEG Encoder 3.1.[01;31m[K53[m[K - '.cue' / '.m3u' Local Buffer Overflow (PoC) | windows/dos/9382.py

Indusoft Thin Client 7.1 - ActiveX Buffer Overflow
| windows/remote/288[01;31m[K53[m[K.html

InduSoft Web Studio 8.1 SP1 - 'Tag Name' Buffer Overflow (SEH)
| windows_x86-64/local/4[01;31m[K53[m[K95.py

Infiltrator Network Security Scanner 4.6 - Denial of Service (PoC)
| windows/dos/4[01;31m[K53[m[K90.py

InfraRecorder 0.[01;31m[K53[m[K - '.txt' Denial of Service (PoC)
| windows_x86/dos/45413.py

InfraRecorder 0.[01;31m[K53[m[K - Memory Corruption (Denial of Service)
| windows/dos/32707.txt

Inout CareerLamp 1.0 Script - Improper Access Restrictions
| php/webapps/410[01;31m[K53[m[K.txt

Inscribe Webmedia - SQL Injection
| php/webapps/17[01;31m[K53[m[K3.txt

```
Installshield 2009 15.0.0.[01;31m[K53[m[K Premier -
'ISWiAutomation15.dll' ActiveX Arbitrary File Overwrite             |
windows/remote/34821.txt

InterAKT Online MX Shop 1.1.1 - SQL Injection
| php/webapps/2[01;31m[K53[m[K23.txt

InterVideo WinDVD 5 - 'cpqdvd.dll' DLL Hijacking
| windows/local/147[01;31m[K53[m[K.c

InTouch Machine Edition 8.1 SP1 - 'Nombre del Tag' Buffer Overflow
(SEH)                                    | windows_x86-
64/local/4[01;31m[K53[m[K78.py

InverseFlow 2.4 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/362[01;31m[K53[m[K.txt

Invision Power Board (IP.Board) 3.0.0b5 - Active Cross-Site Scripting /
Full Path Disclosure               | php/webapps/8[01;31m[K53[m[K8.txt

Invision Power Board 1.x - 'ST' SQL Injection
| php/webapps/2[01;31m[K53[m[K80.txt

Invision Power Board 2.0.1 - 'QPid' SQL Injection
| php/webapps/25[01;31m[K53[m[K5.txt

IObit Uninstaller 9.1.0.8 - 'IObitUnSvr' Unquoted Service Path
| windows/local/47[01;31m[K53[m[K8.txt

iPlanet 4.1 Web Publisher - Remote Buffer Overflow (2)
| multiple/dos/208[01;31m[K53[m[K.php

ISC BIND 8 - Remote Cache Poisoning (1)
| linux/remote/30[01;31m[K53[m[K5.pl

ISC BIND 8 - Remote Cache Poisoning (2)
| linux/remote/30[01;31m[K53[m[K6.pl

ISC BIND 9 - Denial of Service
| multiple/dos/404[01;31m[K53[m[K.py

ISC DHCP 4.x - Multiple Denial of Service Vulnerabilities
| linux/dos/37[01;31m[K53[m[K8.py

iSmartViewPro 1.5 - 'DDNS' Buffer Overflow
| windows_x86/local/4[01;31m[K53[m[K25.py

iSmartViewPro 1.5 - 'SavePath for ScreenShots' Local Buffer Overflow
(SEH)                                    |
windows_x86/local/4[01;31m[K53[m[K49.py

ISPConfig < 3.1.13 - Remote Command Execution
| php/webapps/45[01;31m[K53[m[K4.py
```

```
ItCMS 1.9 - 'boxpop.php' Remote Code Execution
| php/webapps/5[01;31m[K53[m[K2.txt

itech TrainSmart r1044 - SQL injection
| php/webapps/512[01;31m[K53[m[K.txt

jaangle 0.98i.977 - Denial of Service
| windows/dos/35[01;31m[K53[m[K2.py

JAF CMS 4.0 RC2 - Multiple Remote File Inclusions
| php/webapps/[01;31m[K53[m[K17.txt

Jamb - Cross-Site Request Forgery (Add a Post)
| php/webapps/1[01;31m[K53[m[K10.py

Java Applet JMX - Remote Code Execution (Metasploit) (2)
| multiple/remote/24[01;31m[K53[m[K9.rb

Java RMI - Server Insecure Default Configuration Java Code Execution
(Metasploit)                          |
multiple/remote/17[01;31m[K53[m[K5.rb

JBoss JMXInvokerServlet JMXInvoker 0.3 - Remote Command Execution
| java/webapps/365[01;31m[K53[m[K.java

JBoss Seam 2 - Arbitrary File Upload / Execution (Metasploit)
| jsp/remote/366[01;31m[K53[m[K.rb

jCore CMS - Cross-Site Scripting
| php/webapps/10[01;31m[K53[m[K1.txt

JCraft/JSch Java Secure Channel 0.1.[01;31m[K53[m[K - Recursive sftp-
get Directory Traversal                          |
windows/dos/40411.txt

Jenkins Plugin Script Security 1.49/Declarative 1.3.4/Groovy 2.60 -
Remote Code Execution                 |
java/webapps/464[01;31m[K53[m[K.py

jetAudio 7.x - '.m3u' Local Overwrite (SEH)
| windows/local/4[01;31m[K53[m[K1.py

jiNa OCR Image to Text 1.0 - Denial of Service (PoC)
| windows_x86/dos/4[01;31m[K53[m[K80.py

JiRo's FAQ Manager eXperience 1.0 - 'fID' SQL Injection
| asp/webapps/57[01;31m[K53[m[K.txt

JiRos Link Manager 1.0 - 'viewlinks.asp?categoryId' SQL Injection
| asp/webapps/291[01;31m[K53[m[K.txt

JonhCMS 4.5.1 - SQL Injection
| php/webapps/40[01;31m[K53[m[K0.txt
```

Joomla! / Mambo Component Download3000 1.0 - 'id' SQL Injection
| php/webapps/31[01;31m[K53[m[K0.txt

Joomla! 3.2.x < 3.4.4 - SQL Injection
| php/webapps/38[01;31m[K53[m[K4.php

Joomla! 3.4.6 - Remote Code Execution (Metasploit)
| php/webapps/47[01;31m[K53[m[K9.rb

Joomla! Component actualite 1.0 - 'id' SQL Injection
| php/webapps/[01;31m[K53[m[K37.txt

Joomla! Component Ajax Quiz 1.8 - SQL Injection
| php/webapps/42[01;31m[K53[m[K2.txt

Joomla! Component Alphacontent 2.5.8 - 'id' SQL Injection
| php/webapps/[01;31m[K53[m[K10.txt

Joomla! Component Article Factory Manager - Arbitrary File Upload
| php/webapps/12[01;31m[K53[m[K9.txt

Joomla! Component CamelcityDB 2.2 - SQL Injection
| php/webapps/14[01;31m[K53[m[K0.txt

Joomla! Component Cinema 1.0 - SQL Injection
| php/webapps/[01;31m[K53[m[K00.txt

Joomla! Component com_bookJoomlas 0.1 - SQL Injection
| php/webapps/83[01;31m[K53[m[K.txt

Joomla! Component com_digifolio 1.52 - 'id' SQL Injection
| php/webapps/9[01;31m[K53[m[K4.txt

Joomla! Component com_enmasse 5.1 < 6.4 - SQL Injection
| php/webapps/399[01;31m[K53[m[K.txt

Joomla! Component com_hbssearch 1.0 - Blind SQL Injection
| php/webapps/7[01;31m[K53[m[K8.txt

Joomla! Component com_hotbrackets - Blind SQL Injection
| php/webapps/109[01;31m[K53[m[K.txt

Joomla! Component com_jfuploader < 2.12 - Arbitrary File Upload
| php/webapps/1[01;31m[K53[m[K[01;31m[K53[m[K.txt

Joomla! Component com_kunena - 'search' SQL Injection
| php/webapps/221[01;31m[K53[m[K.pl

Joomla! Component com_rsappt_pro2 - Local File Inclusion
| php/webapps/175[01;31m[K53[m[K.txt

Joomla! Component com_sobi2 2.9.3.2 - Blind SQL Injections
| php/webapps/17[01;31m[K53[m[K0.txt

```
Joomla! Component com_tophotelmodule 1.0 - Blind SQL Injection
| php/webapps/7[01;31m[K53[m[K9.txt

Joomla! Component Cookex Agency CKForms - Local File Inclusion
| php/webapps/154[01;31m[K53[m[K.txt

Joomla! Component education - SQL Injection
| php/webapps/121[01;31m[K53[m[K.txt

Joomla! Component FocalPoint 1.2.3 - SQL Injection
| php/webapps/42[01;31m[K53[m[K0.txt

Joomla! Component JoomlaPack 1.0.4a2 RE - 'CAltInstaller.php' Remote
File Inclusion                          |
php/webapps/37[01;31m[K53[m[K.txt

Joomla! Component MyAlbum 1.0 - 'album' SQL Injection
| php/webapps/[01;31m[K53[m[K18.txt

Joomla! Component OnlineFlashQuiz 1.0.2 - Remote File Inclusion
| php/webapps/[01;31m[K53[m[K45.txt

Joomla! Component Price Alert 3.0.2 - 'product_id' SQL Injection
| php/webapps/425[01;31m[K53[m[K.txt

Joomla! Component Pulse Infotech Flip Wall - SQL Injection
| php/webapps/1[01;31m[K53[m[K66.txt

Joomla! Component redSHOP 1.2 - SQL Injection
| php/webapps/27[01;31m[K53[m[K2.txt

Joomla! Component SMEStorage - Local File Inclusion
| php/webapps/118[01;31m[K53[m[K.txt

Joomla! Component Sponsor Wall 1.1 - SQL Injection
| php/webapps/1[01;31m[K53[m[K67.txt

Joomla! Component Turtushout 0.11 - 'Name' SQL Injection
| php/webapps/96[01;31m[K53[m[K.txt

Jorani Leave Management 0.6.5 - (Authenticated) 'startdate' SQL
Injection                                    |
php/webapps/4[01;31m[K53[m[K40.txt

Jorani Leave Management 0.6.5 - Cross-Site Scripting
| php/webapps/4[01;31m[K53[m[K38.txt

JourneyMap 5.0.0RC2 Ultimate Edition - Resource Consumption (Denial of
Service)                                |
multiple/dos/3[01;31m[K53[m[K39.txt

jPORTAL 2.3.1 - 'Banner.php' SQL Injection
| php/webapps/2[01;31m[K53[m[K82.txt
```

JShop 1.x < 2.x - 'xPage' Local File Inclusion
| php/webapps/[01;31m[K53[m[K25.txt

Kandidat CMS 1.4.2 - Persistent Cross-Site Scripting
| php/webapps/1[01;31m[K53[m[K85.txt

Kaspersky 2010 - Remote Memory Corruption / Denial of Service (PoC)
| windows/dos/9[01;31m[K53[m[K7.html

KaZaA Media Desktop 1.7.1 - Large Message Denial of Service
| windows/dos/216[01;31m[K53[m[K.c

KDE 4/5 - 'KAuth' Local Privilege Escalation
| linux/local/420[01;31m[K53[m[K.c

KDE KMail 1.7.1 - HTML EMail Remote Email Content Spoofing
| linux/remote/2[01;31m[K53[m[K75.pl

Kerio Personal Firewall 2.1.4 - Remote Authentication Packet Overflow
(Metasploit) |
windows/remote/1[01;31m[K53[m[K7.pm

KeystoneJS 4.0.0-beta.5 - CSV Excel Macro Injection
| nodejs/webapps/430[01;31m[K53[m[K.txt

KingView 6.[01;31m[K53[m[K - 'KChartXY' ActiveX File Creation /
Overwrite |
windows/local/28085.html

KingView 6.[01;31m[K53[m[K - 'SuperGrid' Insecure ActiveX Control
| windows/local/28084.html

Kingview Touchview 6.[01;31m[K53[m[K - EIP Overwrite
| windows/dos/19388.py

Kingview Touchview 6.[01;31m[K53[m[K - Multiple Heap Overflow
Vulnerabilities |
windows/dos/19389.txt

KISGB (tmp_theme) 5.1.1 - Local File Inclusion
| php/webapps/[01;31m[K53[m[K24.txt

Kleophatra CMS 0.1.1 - 'module' Cross-Site Scripting
| php/webapps/338[01;31m[K53[m[K.txt

KMPlayer 2.9.3.1214 - '.ksf' Remote Buffer Overflow
| multiple/remote/3[01;31m[K53[m[K98.pl

KomSeo Cart 1.3 - 'my_item_search' SQL Injection
| php/webapps/447[01;31m[K53[m[K.txt

Kroum Grigorov KpyM Telnet Server 1.0 - Remote Denial of Service
| windows/dos/23[01;31m[K53[m[K0.c

Kubernetes - (Authenticated) Arbitrary Requests
| multiple/remote/460[01;31m[K53[m[K.py

KwsPHP 1.3.456 Module Archives - 'id' SQL Injection
| php/webapps/[01;31m[K53[m[K51.txt

KwsPHP 1.3.456 Module Galerie - 'id_gal' SQL Injection
| php/webapps/[01;31m[K53[m[K50.txt

KwsPHP Module ConcoursPhoto 2.0 - 'C_ID' SQL Injection
| php/webapps/[01;31m[K53[m[K[01;31m[K53[m[K.txt

KwsPHP Module jeuxflash 1.0 - 'cat' SQL Injection
| php/webapps/[01;31m[K53[m[K52.txt

Kyocera Printer d-COPIA2[01;31m[K53[m[KMF - Directory Traversal (PoC)
| hardware/webapps/48561.txt

LAMS < 3.1 - Cross-Site Scripting
| java/webapps/451[01;31m[K53[m[K.txt

Lan Messenger - sending PM 'UNICODE' Overwrite Buffer Overflow (SEH)
| windows/dos/2[01;31m[K53[m[K63.py

Land Down Under 800/801 - 'auth.php?m' SQL Injection
| php/webapps/262[01;31m[K53[m[K.txt

LANDesk Management Suite 8.7 Alert Service - 'AOLSRVR.exe' Remote
Buffer Overflow |
windows/remote/298[01;31m[K53[m[K.rb

LayerBB Forum 1.1.1 - 'search_query' SQL Injection
| php/webapps/45[01;31m[K53[m[K0.txt

LeadTools MultiMedia 15 - 'LTMM15.dll' ActiveX Control Arbitrary File
Overwrite |
windows/remote/31[01;31m[K53[m[K4.html

Leawo Prof. Media 11.0.0.1 - Denial of Service (DoS) (PoC)
| windows/dos/501[01;31m[K53[m[K.py

LetoDms 1.4.x - 'lang' Local File Inclusion
| php/webapps/33[01;31m[K53[m[K0.txt

LG G4 - Touchscreen Driver write_log Kernel Read/Write
| android/dos/413[01;31m[K53[m[K.txt

LG Smart IP Camera 1508190 - Backup File Download
| hardware/webapps/4[01;31m[K53[m[K94.py

LibLime Koha 4.2 - Local File Inclusion
| cgi/webapps/181[01;31m[K53[m[K.txt

```
Libopt.a 3.1x - Error Logging Buffer Overflow (1)
| linux/dos/22[01;31m[K53[m[K7.c

Libopt.a 3.1x - Error Logging Buffer Overflow (2)
| linux/local/22[01;31m[K53[m[K8.pl

LibreNMS 1.46 - 'search' SQL Injection
| multiple/webapps/484[01;31m[K53[m[K.txt

libvirt_proxy 0.5.1 - Local Privilege Escalation
| linux/local/8[01;31m[K53[m[K4.c

Lighthouse Development Squirrelcart 1.5.5 - SQL Injection
| php/webapps/2[01;31m[K53[m[K20.txt

Links Directory 1.1 - 'cat_id' SQL Injection
| php/webapps/[01;31m[K53[m[K77.txt

Linksys WAG54G v2 Wireless ADSL Router - HTTPd Denial of Service
| hardware/dos/7[01;31m[K53[m[K5.php

Linksys WET11 - Password Update Remote Authentication Bypass
| hardware/remote/2[01;31m[K53[m[K59.txt

Linksys WRT54G Firmware 1.00.9 - Security Bypass (1)
| hardware/remote/[01;31m[K53[m[K13.txt

LinPHA 1.3.3 Plugin Maps - Remote Command Execution
| php/webapps/[01;31m[K53[m[K92.php

Linux 4.4.0 < 4.4.0-[01;31m[K53[m[K - 'AF_PACKET chocobo_root' Local
Privilege Escalation (Metasploit)                  |
linux/local/44696.rb

Linux Kernel - 'AF_PACKET' Use-After-Free (2)
| linux/dos/440[01;31m[K53[m[K.md

Linux Kernel 2.2.x/2.3/2.4.x - 'd_path()' Path Truncation
| linux/local/213[01;31m[K53[m[K.c

Linux Kernel 2.6 - Console Keymap Local Command Injection
| linux/local/263[01;31m[K53[m[K.txt

Linux Kernel 2.6.10 - File Lock Local Denial of Service
| linux/dos/2[01;31m[K53[m[K22.c

Linux Kernel 2.6.36 - VIDIOCSMICROCODE IOCTL Local Memory Overwrite
| linux/local/1[01;31m[K53[m[K44.c

Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'digi_acceleport' Nullpointer
Dereference                         | linux/dos/39[01;31m[K53[m[K7.txt
```

```
Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - 'Wacom' Multiple Nullpointer
Dereferences                          | linux/dos/39[01;31m[K53[m[K8.txt

Linux Kernel 3.10.0 (CentOS / RHEL 7.1) - visor 'treo_attach'
Nullpointer Dereference                              |
linux/dos/39[01;31m[K53[m[K9.txt

Linux Kernel 3.14.5 (CentOS 7 / RHEL) - 'libfutex' Local Privilege
Escalation                                    |
linux/local/3[01;31m[K53[m[K70.c

Linux Kernel < 4.11.8 - 'mq_notify: double sock_put()' Local Privilege
Escalation                            | linux/local/455[01;31m[K53[m[K.c

LionMax Software WWW File Share Pro 2.4/2.6 - Remote Denial of Service
| windows/dos/23[01;31m[K53[m[K8.txt

Litespeed 2.1.5 - 'ConfMgr.php' Cross-Site Scripting
| php/webapps/26[01;31m[K53[m[K5.txt

Logics Software LOG-FT - Arbitrary File Disclosure
| windows/remote/2[01;31m[K53[m[K36.txt

Logicspice FAQ Script 2.9.7 - Remote Code Execution
| php/webapps/4[01;31m[K53[m[K26.txt

Logwatch Log File - Special Characters Privilege Escalation
| linux/remote/3[01;31m[K53[m[K86.txt

Lotus Domino Server 5.0.x - Directory Traversal (2)
| multiple/remote/20[01;31m[K53[m[K0.sh

Luch Web Designer - Multiple SQL Injections
| asp/webapps/169[01;31m[K53[m[K.txt

LW-N605R 12.20.2.1486 - Remote Code Execution
| hardware/webapps/4[01;31m[K53[m[K51.py

Lynx 2.8 - '.mailcap'/'.mime.type' Local Code Execution
| linux/remote/32[01;31m[K53[m[K0.txt

Mabry Software FTPServer/X 1.0 - Controls Format String
| linux/dos/23[01;31m[K53[m[K9.txt

Macaron Notes great notebook 5.5 - Denial of Service (PoC)
| ios/dos/499[01;31m[K53[m[K.py

Machform Form Maker 2 - Multiple Vulnerabilities
| php/webapps/265[01;31m[K53[m[K.txt

Macromedia JRun 3/4 JSP Engine - Denial of Service
| windows/dos/21[01;31m[K53[m[K6.jsp
```

```
mailtraq 2.17.3.3150 - Persistent Cross-Site Scripting
| windows/webapps/203[01;31m[K53[m[K.py

Mailtraq 2.x - Administration Console Privilege Escalation
| windows/local/247[01;31m[K53[m[K.txt

MakeBook 2.2 - Form Field Input Validation
| cgi/webapps/21[01;31m[K53[m[K5.txt

maluinfo 206.2.38 - 'bb_usage_stats.php' Remote File Inclusion
| php/webapps/2[01;31m[K53[m[K7.pl

Mambo Component Ahsshop 1.51 - 'vara' SQL Injection
| php/webapps/[01;31m[K53[m[K35.txt

Mambo Component nfnaddressbook 0.4 - Remote File Inclusion
| php/webapps/3[01;31m[K53[m[K9.txt

Mambo Open Source 4.5/4.6 - 'mod_mainmenu.php' Remote File Inclusion
| php/webapps/235[01;31m[K53[m[K.php

Mambo Open Source 4.6.2 - '/mambots/editors/mostlyce/'
PHP/connector.php?Query String Cross-Site Scripting |
php/webapps/322[01;31m[K53[m[K.txt

ManageEngine ADSelfService Plus 4.4 - 'EmployeeSearch.cc' Multiple
Cross-Site Scripting Vulnerabilities    |
php/webapps/3[01;31m[K53[m[K31.txt

ManageEngine ADSelfService Plus 4.4 - POST Manipulation Security
Question                                  |
php/webapps/3[01;31m[K53[m[K30.txt

ManageEngine Exchange Reporter Plus < Build [01;31m[K53[m[K11 - Remote
Code Execution                                  |
java/webapps/44975.py

Maran PHP Shop - 'prod.php' SQL Injection
| php/webapps/69[01;31m[K53[m[K.txt

Marinet CMS - 'gallery.php?id' SQL Injection
| php/webapps/36[01;31m[K53[m[K6.txt

Marinet CMS - 'galleryphoto.php?id' SQL Injection
| php/webapps/36[01;31m[K53[m[K5.txt

Marinet CMS - 'room2.php?roomid' SQL Injection
| php/webapps/36[01;31m[K53[m[K4.txt

MauryCMS 0.[01;31m[K53[m[K.2 - Arbitrary File Upload
| php/webapps/7162.pl
```

```
Maxthon 3.0.18.1000 - CSS Denial of Service
| windows/dos/1[01;31m[K53[m[K94.txt

Maxtrade AIO 1.3.23 - 'categori' SQL Injection
| php/webapps/58[01;31m[K53[m[K.txt

McAfee Data Loss Prevention Endpoint - Arbitrary Write Privilege
Escalation                                |
windows/local/359[01;31m[K53[m[K.c

Mcafee EPO 4.0 - 'FrameworkService.exe' Remote Denial of Service
| windows/dos/[01;31m[K53[m[K43.py

McAfee VirusScan Enterprise 8.8 - Security Restrictions Bypass
| windows/local/39[01;31m[K53[m[K1.c

McAfee Visual Trace - ActiveX Control Buffer Overflow (Metasploit)
| windows/remote/16[01;31m[K53[m[K8.rb

MDPro 1.0.76 - 'index.php' SQL Injection
| php/webapps/29[01;31m[K53[m[K7.txt

MedDream PACS Server 6.8.3.751 - Remote Code Execution (Authenticated)
| php/webapps/488[01;31m[K53[m[K.py

MedDream PACS Server Premium 6.7.1.1 - 'email' SQL Injection
| php/webapps/4[01;31m[K53[m[K44.txt

Media Player Classic 6.4.9.1 - '.avi' Buffer Overflow
| windows/dos/11[01;31m[K53[m[K5.pl

Mediacoder 0.7.3.4682 - Universal Buffer Overflow (SEH)
| windows/local/141[01;31m[K53[m[K.pl

Mediacoder 0.8.33 build 5680 - '.lst' Buffer Overflow (PoC) (SEH
Overwrite)                                |
windows/dos/35[01;31m[K53[m[K1.py

Mediacoder 0.8.33 build 5680 - '.m3u' Buffer Overflow (PoC) (SEH
Overwrite)                                |
windows/dos/35[01;31m[K53[m[K0.py

MediaSlash Gallery - 'index.php' Remote File Inclusion
| php/webapps/27[01;31m[K53[m[K4.txt

MediaTek Wirless Utility rt2870 - Denial of Service (PoC)
| windows/dos/4[01;31m[K53[m[K98.py

MemHT Portal 4.0.1 - Persistent Cross-Site Scripting
| php/webapps/1[01;31m[K53[m[K86.txt
```

Mercur Messaging 2005 (Windows 2000 SP4) - IMAP 'Subscribe' Remote Overflow |
windows/remote/3[01;31m[K53[m[K7.py

MercuryBoard 1.1.5 - 'login.php' Blind SQL Injection
| php/webapps/56[01;31m[K53[m[K.php

MetaCart E-Shop V-8 - 'IntProdID' SQL Injection
| asp/webapps/25[01;31m[K53[m[K6.txt

MetaCart E-Shop V-8 - 'StrCatalog_NAME' SQL Injection
| asp/webapps/25[01;31m[K53[m[K7.txt

MetaCart2 - 'IntCatalogID' SQL Injection
| asp/webapps/25[01;31m[K53[m[K9.txt

MetInfo 2.0 - PHP Code Injection
| php/webapps/1[01;31m[K53[m[K60.pl

MetInfo 3.0 - 'FCKeditor' Arbitrary File Upload
| php/webapps/1[01;31m[K53[m[K89.php

MetInfo 3.0 - PHP Code Injection
| php/webapps/1[01;31m[K53[m[K61.pl

Mewsoft NetAuction 3.0 - Cross-Site Scripting
| cgi/webapps/215[01;31m[K53[m[K.txt

MG2 0.5.1 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K53[m[K48.txt

Microsoft Baseline Security Analyzer 2.3 - XML External Entity Injection |
windows/local/4[01;31m[K53[m[K54.txt

Microsoft BizTalk Server 2002 - HTTP Receiver Buffer Overflow
| windows/dos/225[01;31m[K53[m[K.txt

Microsoft Credential Security Support Provider - Remote Code Execution
| windows/remote/444[01;31m[K53[m[K.md

Microsoft Edge Chakra JIT - Bound Check Elimination Bug
| windows/dos/446[01;31m[K53[m[K.js

Microsoft Edge Chakra: JIT - 'Lowerer::LowerBoundCheck' Incorrect Integer Overflow Check |
windows/dos/431[01;31m[K53[m[K.js

Microsoft Exchange 2019 15.2.221.12 - Authenticated Remote Code Execution |
windows/remote/481[01;31m[K53[m[K.py

Microsoft FrontPage Personal Web Server 1.0/4.0 - Directory Traversal | windows/remote/197[01;31m[K53[m[K.txt

Microsoft IIS 7.0 FTP Server - Stack Exhaustion Denial of Service (MS09-0[01;31m[K53[m[K) (Metasploit) | windows/dos/17476.rb

Microsoft IIS FTP Server - NLST Response Overflow (MS09-0[01;31m[K53[m[K) (Metasploit) | windows/remote/16740.rb

Microsoft Internet Explorer - '.ANI' Remote Stack Overflow (MS05-002) (2) | windows/remote/7[01;31m[K53[m[K.html

Microsoft Internet Explorer - CSS Recursive Import Use-After-Free (MS11-003) (Metasploit) | windows/remote/16[01;31m[K53[m[K3.rb

Microsoft Internet Explorer - MSHTML!CMultiReadStreamLifetimeManager::ReleaseThreadStateInternal Read AV | windows/dos/402[01;31m[K53[m[K.html

Microsoft Internet Explorer - SLayoutRun Use-After-Free (MS13-009) (Metasploit) (2) | windows/remote/24[01;31m[K53[m[K8.rb

Microsoft Internet Explorer - XML Core Services HTTP Request Handling (MS06-071) (Metasploit) | windows/remote/16[01;31m[K53[m[K2.rb

Microsoft Internet Explorer 11 - 'Js::RegexHelper::RegexReplace' Use-After-Free | windows/dos/441[01;31m[K53[m[K.html

Microsoft Internet Explorer 5 - Download Behaviour | windows/remote/19[01;31m[K53[m[K0.txt

Microsoft Internet Explorer 5 - Remote 'URLMON.dll' Remote Buffer Overflow | windows/remote/22[01;31m[K53[m[K0.pl

Microsoft Internet Explorer 5.0.1 - Content Advisor File Handling Buffer Overflow (MS05-020) | windows/remote/2[01;31m[K53[m[K85.cpp

Microsoft Internet Explorer 5.0.1 - DHTML Object Race Condition Memory Corruption | windows/remote/2[01;31m[K53[m[K86.txt

```
Microsoft Internet Explorer 5.0.1 - Multiple ActiveX Controls Denial of
Service Vulnerabilities            |
windows/dos/29[01;31m[K53[m[K6.html

Microsoft Internet Explorer 5.0/4.0.1 - iFrame
| windows/remote/19[01;31m[K53[m[K9.txt

Microsoft Internet Explorer 6 - ' ' Address Bar URI Spoofing
| php/webapps/32[01;31m[K53[m[K9.html

Microsoft Internet Explorer 6.0 SP0 - IsComponentInstalled() Remote
(Metasploit)                              |
windows/remote/1[01;31m[K53[m[K6.pm

Microsoft Internet Explorer 6/7 - XML Core Services Remote Code
Execution (3)                             |
windows/remote/27[01;31m[K53[m[K.c

Microsoft Internet Explorer 7/8 - findText Unicode Parsing Crash
| windows/dos/92[01;31m[K53[m[K.html

Microsoft Internet Explorer OLE Pre-IE11 - Automation Array Remote Code
Execution / PowerShell VirtualAllo |
windows/remote/3[01;31m[K53[m[K08.html

Microsoft MSN Messenger 8.0 - Video Conversation Buffer Overflow
| windows/remote/30[01;31m[K53[m[K7.txt

Microsoft Office Web Components (OWC) Spreadsheet - msDataSourceObject
Memory Corruption (MS09-043) (Metas |
windows/remote/16[01;31m[K53[m[K7.rb

Microsoft Office XP SP3 - '.PPT' File Buffer Overflow (MS08-016)
| windows/local/[01;31m[K53[m[K20.txt

Microsoft OneNote (Version 2305 Build 16.0.16501.20074) 64-bit -
Spoofing                                  |
multiple/remote/51[01;31m[K53[m[K8.txt

Microsoft People 10.1807.2131.0 - Denial of service (PoC)
| windows_x86-64/dos/4[01;31m[K53[m[K35.txt

Microsoft SharePoint - Deserialization Remote Code Execution
| windows/remote/480[01;31m[K53[m[K.py

Microsoft Visual InterDev 6.0 SP6 - '.sln' Local Buffer Overflow (PoC)
| windows/dos/[01;31m[K53[m[K49.py

Microsoft Windows - '.reg' File / Dialog Box Message Spoofing
| windows/dos/46[01;31m[K53[m[K3.txt

Microsoft Windows - 'SMBGhost' Remote Code Execution
| windows/remote/48[01;31m[K53[m[K7.py
```

```
Microsoft Windows - 'win32k.sys' Denial of Service
| windows/dos/3[01;31m[K53[m[K26.cpp

Microsoft Windows - ASN.1 'LSASS.exe' Remote Denial of Service (MS04-
007)                                  | windows/dos/1[01;31m[K53[m[K.c

Microsoft Windows - DCE-RPC svcctl ChangeServiceConfig2A() Memory
Corruption                                |
windows/dos/34[01;31m[K53[m[K.py

Microsoft Windows - Multiple UAC Protection Bypasses
| windows/local/477[01;31m[K53[m[K.md

Microsoft Windows - NTUserMessageCall Win32k Kernel Pool Overflow
'schlamperei.x86.dll' (MS13-0[01;31m[K53[m[K) (Metasp |
windows_x86/local/33213.rb

Microsoft Windows - SetImeInfoEx Win32k NULL Pointer Dereference
(Metasploit)                              |
windows/local/456[01;31m[K53[m[K.rb

Microsoft Windows - Uniscribe Font Processing Heap Memory Corruption
Around 'USP10!BuildFSM' (MS17-011)    |
windows/dos/416[01;31m[K53[m[K.txt

Microsoft Windows .Reg File - Dialog Spoof / Mitigation Bypass
| windows/local/506[01;31m[K53[m[K.txt

Microsoft Windows 10 - 'pcap' Driver Privilege Escalation
| windows/local/38[01;31m[K53[m[K3.c

Microsoft Windows 10 AppXSvc Deployment Service - Arbitrary File
Deletion                                  |
windows/local/472[01;31m[K53[m[K.cpp

Microsoft Windows Explorer - '.doc' File Denial of Service
| windows/dos/[01;31m[K53[m[K27.txt

Microsoft Windows Explorer Out-of-Bound Read - Denial of Service (PoC)
| windows/dos/4[01;31m[K53[m[K20.py

Microsoft Windows Media Encoder (XP SP2) - 'wmex.dll' ActiveX Buffer
Overflow (MS08-0[01;31m[K53[m[K)                  |
windows/remote/6454.html

Microsoft Windows Media Encoder 9 - 'wmex.dll' ActiveX Buffer Overflow
(MS08-0[01;31m[K53[m[K) (Metasploit)             |
windows/remote/16521.rb

Microsoft Windows Media Player 11.0.5721.5145 - '.avi' Buffer Overflow
| windows/dos/355[01;31m[K53[m[K.pl
```

```
Microsoft Windows Media Player 11.0.5721.5145 - '.mpg' Buffer Overflow
| windows/dos/11[01;31m[K53[m[K1.pl

Microsoft Windows Media Player 7.0 - '.wmz' Arbitrary Java Applet
| windows/remote/205[01;31m[K53[m[K.html

Microsoft Windows Metafile - 'gdi32.dll' Denial of Service (MS05-
0[01;31m[K53[m[K                                          |
windows/dos/1343.c

Microsoft Windows Metafile - 'mtNoObjects' Denial of Service (MS05-
0[01;31m[K53[m[K                                         |
windows/dos/1346.c

Microsoft Windows MSHTML Engine - 'Edit' Remote Code Execution
| windows/local/46[01;31m[K53[m[K6.txt

Microsoft Windows Task Scheduler (XP/2000) - '.job' (MS04-022)
| windows/local/3[01;31m[K53[m[K.c

Microsoft Windows XP/2000 - Internet Protocol Validation Remote Code
Execution (1)                          |
windows/dos/2[01;31m[K53[m[K83.pl

Microsoft Windows XP/2000 - Internet Protocol Validation Remote Code
Execution (2)                          |
windows/remote/2[01;31m[K53[m[K84.c

Microsoft Windows XP/2000/NT 4.0 - RPC Service Denial of Service (3)
| windows/dos/219[01;31m[K53[m[K.txt

Microsoft Works 7 - 'WkImgSrv.dll' ActiveX Remote Buffer Overflow
| windows/remote/5[01;31m[K53[m[K0.html

Millewin 13.39.146.1 - Local Privilege Escalation
| windows/local/49[01;31m[K53[m[K0.txt

MinaliC WebServer 1.0 - Denial of Service
| windows/dos/1[01;31m[K53[m[K34.py

MinaliC WebServer 1.0 - Directory Traversal
| windows/remote/1[01;31m[K53[m[K33.txt

MinaliC WebServer 1.0 - Remote Source Disclosure / File Download
| windows/remote/1[01;31m[K53[m[K36.txt

minewebcms 1.15.2 - Cross-site Scripting (XSS)
| php/webapps/508[01;31m[K53[m[K.txt

Mini-stream RM-MP3 Converter 3.1.2.1.2010.03.30 - '.wax' Local Buffer
Overflow (SEH)                         |
windows/local/3[01;31m[K53[m[K77.rb
```

```
Mini-stream RM-MP3 Converter/WMDownloader/ASX to MP3 Converter - Local
Stack Buffer Overflow               |
windows/local/14[01;31m[K53[m[K2.py

Minix 3.3.0 - Remote TCP/IP Stack Denial of Service
| linux/dos/3[01;31m[K53[m[K02.c

mIRC - IRC URL Buffer Overflow (Metasploit)
| windows/remote/16[01;31m[K53[m[K0.rb

MNOGoSearch 3.1.20 - 'search.cgi?UL' Remote Buffer Overflow (1)
| cgi/remote/227[01;31m[K53[m[K.pl

MobileCartly 1.0 - Arbitrary File Upload
| php/webapps/20[01;31m[K53[m[K9.txt

Moby NetSuite 1.0/1.2 - POST Handler Buffer Overflow
| multiple/dos/220[01;31m[K53[m[K.txt

MOC Designs PHP News 1.1 - Authentication Bypass
| php/webapps/93[01;31m[K53[m[K.txt

Modbus Slave 7.3.1 - Buffer Overflow (DoS)
| windows/dos/50[01;31m[K53[m[K6.py

ModernGigabyte ModernBill 4.3 - 'Aid' Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K78.txt

ModernGigabyte ModernBill 4.3 - 'C_CODE' Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K77.txt

ModernGigabyte ModernBill 4.3 - 'news.php' File Inclusion
| php/webapps/2[01;31m[K53[m[K76.txt

mod_accounting Module 0.5 - Blind SQL Injection
| linux/webapps/286[01;31m[K53[m[K.txt

MoinMoin - Arbitrary Command Execution
| php/webapps/2[01;31m[K53[m[K04.py

Mole 2.1.0 - 'viewsource.php' Remote File Disclosure
| php/webapps/[01;31m[K53[m[K94.txt

Mongoose Web Server 2.11 - Directory Traversal
| windows/remote/1[01;31m[K53[m[K73.txt

Monster Top List 1.4.2 - 'functions.php?root_path' Remote File
Inclusion                                |
php/webapps/3[01;31m[K53[m[K0.pl

MooPlayer 1.3.0 - 'm3u' Local Buffer Overflow (SEH) (1)
| windows/local/360[01;31m[K53[m[K.py
```

```
mooSocial Store Plugin 2.6 - SQL Injection
| php/webapps/4[01;31m[K53[m[K30.txt

Motorola Timbuktu Pro 8.6.3.1367 - Directory Traversal
| windows/remote/30[01;31m[K53[m[K2.pl

MoviePlay 4.82 - '.lst' Local Buffer Overflow
| windows/local/161[01;31m[K53[m[K.py

Moxa EDR-810 - Command Injection / Information Disclosure
| hardware/remote/47[01;31m[K53[m[K6.txt

Mozilla Firefox - Interleaving 'document.write' / 'appendChild' Denial
of Service                          |
multiple/dos/1[01;31m[K53[m[K41.html

Mozilla Firefox - Simplified Memory Corruption (PoC)
| multiple/dos/1[01;31m[K53[m[K42.html

Mozilla Firefox 1.0.7 / Thunderbird 1.0.6 - Denial of Service
| multiple/dos/12[01;31m[K53[m[K.html

Mozilla Firefox 1.0.x/1.5 - HTML Parsing Denial of Service
| linux/dos/272[01;31m[K53[m[K.txt

Mozilla Firefox 3.6.8 < 3.6.11 - Interleaving 'document.write' /
'appendChild' Remote Overflow             |
windows/remote/1[01;31m[K53[m[K52.html

Mozilla Firefox 4.0.1 - 'Array.reduceRight()' Remote Overflow
| windows/remote/18[01;31m[K53[m[K1.html

Mozilla Firefox 49.0.1 - Denial of Service
| windows/dos/40[01;31m[K53[m[K6.py

Mozilla Firefox < [01;31m[K53[m[K - 'ConvolvePixel' Memory Disclosure
| multiple/dos/42072.html

Mozilla Firefox < [01;31m[K53[m[K - 'gfxTextRun' Out-of-Bounds Read
| multiple/dos/42071.html

Mozilla Suite/Firefox - JavaScript Lambda Replace Heap Memory
Disclosure                                  |
linux/dos/2[01;31m[K53[m[K34.txt

MPCS 1.0 - 'path' Remote File Inclusion
| php/webapps/26[01;31m[K53[m[K.txt

MPlayer 0.9/1.0 - MMST Get_Header Remote Client-Side Buffer Overflow
| linux/remote/248[01;31m[K53[m[K.c
```

MPlayer 1.0 rc2 - 'sdpplin_parse()' Array Indexing Buffer Overflow (PoC) | linux/dos/[01;31m[K53[m[K07.pl

Mpxplay MultiMedia Commander 2.00a - '.m3u' Stack Buffer Overflow (PoC) | windows/dos/380[01;31m[K53[m[K.txt

Multiple Check Point Endpoint Security Products - Information Disclosure | hardware/remote/3[01;31m[K53[m[K17.txt

Multiple Vendor BIOS - Keyboard Buffer Password Persistence (2) | unix/local/267[01;31m[K53[m[K.c

Multiple Vendor ICMP Implementation - Malformed Path MTU Denial of Service | multiple/dos/2[01;31m[K53[m[K88.txt

Multiple Vendor ICMP Implementation - Spoofed Source Quench Packet Denial of Service | multiple/dos/2[01;31m[K53[m[K87.txt

Multiple Vendor ICMP Message Handling - Denial of Service | multiple/dos/2[01;31m[K53[m[K89.txt

Multiple Vendor Telnet Client - Env_opt_add Heap Buffer Overflow | linux/dos/2[01;31m[K53[m[K03.txt

Multireligion Responsive Matrimonial Script 4.7.1 - SQL Injection | php/webapps/41[01;31m[K53[m[K0.txt

mxBB Module mx_blogs 2.0.0-beta - Remote File Inclusion | php/webapps/[01;31m[K53[m[K23.pl

My Databook - 'diary.php?year' Cross-Site Scripting | php/webapps/301[01;31m[K53[m[K.txt

My Image Gallery 1.4.1 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/261[01;31m[K53[m[K.txt

MyBB 1.4.2 - 'moderation.php' Cross-Site Scripting | php/webapps/32[01;31m[K53[m[K5.txt

MyBB 1.6 - Full Path Disclosure | php/webapps/1[01;31m[K53[m[K25.txt

MyBB 1.8.17 - Cross-Site Scripting | php/webapps/4[01;31m[K53[m[K93.txt

MyBB 1.8.2 - 'unset_globals()' Function Bypass / Remote Code Execution | php/webapps/3[01;31m[K53[m[K23.md

MyBB Plugin Custom Pages 1.0 - SQL Injection
| php/webapps/[01;31m[K53[m[K79.txt

MyBB User Social Networks Plugin 1.2 - Persistent Cross-Site Scripting
| php/webapps/34[01;31m[K53[m[K9.txt

MyBlog 0.9.8 - Insecure Cookie Handling
| php/webapps/6[01;31m[K53[m[K1.txt

MyBulletinBoard (MyBB) 1.03 - 'misc.php' SQL Injection
| php/webapps/1[01;31m[K53[m[K9.txt

MyBulletinBoard (MyBB) 1.2.3 - Remote Code Execution
| php/webapps/36[01;31m[K53[m[K.php

mycart 2.0 - Multiple Vulnerabilities
| php/webapps/1[01;31m[K53[m[K40.txt

mygamingladder MGL Combo System 7.5 - 'game.php' SQL Injection
| php/webapps/1[01;31m[K53[m[K51.rb

Myiosoft EasyBookMarker 4 - 'Parent' SQL Injection
| php/webapps/70[01;31m[K53[m[K.txt

MyIT CRM - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/14[01;31m[K53[m[K1.txt

MyMp3 Player Stack - '.m3u' File DEP Bypass
| windows/local/200[01;31m[K53[m[K.py

mySeatXT 0.164 - 'lang' Local File Inclusion
| php/webapps/3[01;31m[K53[m[K76.txt

MySQL 6.0 yaSSL 1.7.5 - Hello Message Buffer Overflow (Metasploit)
| linux/remote/99[01;31m[K53[m[K.rb

MyYoutube MyBB Plugin 1.0 - SQL Injection
| php/webapps/233[01;31m[K53[m[K.txt

Neat weblog 0.2 - 'articleId' SQL Injection
| php/webapps/[01;31m[K53[m[K31.pl

NEC UNIVERGE UM4730 < 11.8 - SQL Injection
| php/webapps/423[01;31m[K53[m[K.txt

Nero Burning ROM 9.4.13.2 - ISO Compilation Local Buffer Invasion (PoC)
| windows/dos/11[01;31m[K53[m[K3.pl

NetBSD 5.0 - Hack PATH Environment Overflow (PoC)
| netbsd_x86/dos/126[01;31m[K53[m[K.sh

NETGATE Registry Cleaner 16.0.205 - Unquoted Service Path Privilege Escalation |
windows/local/40[01;31m[K53[m[K9.txt

Netgear FM114P ProSafe Wireless Router - UPnP Information Disclosure
| hardware/remote/224[01;31m[K53[m[K.txt

Netgear WNR500 Wireless Router - 'webproc?getpage' Traversal Arbitrary File Access |
hardware/webapps/3[01;31m[K53[m[K25.txt

Netis ADSL Router DL4322D RTK 2.1.1 - Cross-Site Request Forgery (Add Admin) |
hardware/webapps/45[01;31m[K53[m[K2.txt

Netis E1+ 1.2.32[01;31m[K53[m[K3 - Backdoor Account (root)
| hardware/webapps/48382.txt

Netis E1+ V1.2.32[01;31m[K53[m[K3 - Unauthenticated WiFi Password Leak
| hardware/webapps/48384.txt

Netscape 4.x/6.x / Mozilla 0.9.x - Malformed Email POP3 Denial of Service |
multiple/dos/21[01;31m[K53[m[K9.c

NetSetMan 4.7.1 - Local Buffer Overflow (SEH Unicode)
| windows/local/46[01;31m[K53[m[K0.py

NetWin DBabble 2.5 i - Cross-Site Scripting
| cgi/webapps/231[01;31m[K53[m[K.txt

Network Community Script 3.0.2 - SQL Injection
| php/webapps/41[01;31m[K53[m[K1.txt

Network Manager VPNC 1.2.6 - 'Username' Local Privilege Escalation (Metasploit) |
linux/local/4[01;31m[K53[m[K13.rb

NetworkActiv Web Server 4.0 Pre-Alpha-3.7.2 - 'Username' Denial of Service (PoC) | windows_x86-
64/dos/4[01;31m[K53[m[K02.py

NetworkSleuth 3.0.0.0 - 'Key' Denial of Service (PoC)
| windows/dos/478[01;31m[K53[m[K.py

NICO-FTP 3.0.1.19 - Buffer Overflow (SEH) (ASLR Bypass)
| windows_x86/local/45[01;31m[K53[m[K1.py

NinkoBB 1.3RC5 - Cross-Site Scripting
| php/webapps/1[01;31m[K53[m[K30.txt

NitroSecurity ESM 8.4.0a - Remote Code Execution
| linux/remote/1[01;31m[K53[m[K18.txt

NO-IP DUC 4.1.1 - Unquoted Service Path Privilege Escalation
| windows/local/40[01;31m[K53[m[K3.txt

Nokia ASIKA 7.13.52 - Hard-coded private key disclosure
| hardware/remote/51[01;31m[K53[m[K5.c

Nokia IPSO 3.4.x - Voyager ReadFile.TCL Remote File Reading
| hardware/remote/22[01;31m[K53[m[K3.txt

NolaPro Enterprise 4.0.5[01;31m[K53[m[K8 - Cross-Site Scripting / SQL Injection |
php/webapps/33919.txt

Nord VPN 6.14.31 - Denial of Service (PoC)
| windows_x86-64/dos/4[01;31m[K53[m[K04.py

Notes Manager 1.0 - Arbitrary File Upload
| php/webapps/457[01;31m[K53[m[K.txt

Noticeware Email Server 4.6.1.0 - Denial of Service
| windows/dos/[01;31m[K53[m[K41.pl

Novaboard 1.1.4 - Local File Inclusion
| php/webapps/1[01;31m[K53[m[K24.txt

NovaRad NovaPACS Diagnostics Viewer 8.5 - XML External Entity Injection (File Disclosure) | xml/webapps/4[01;31m[K53[m[K37.txt

Novel eDirectory HTTP - Denial of Service
| windows/dos/[01;31m[K53[m[K44.py

Novell eDirectory 8.8 and Netware LDAP-SSL Daemon - Denial of Service
| multiple/dos/357[01;31m[K53[m[K.pl

Novell eDirectory 8.x - eMBox Utility 'edirutil' Command
| novell/remote/31[01;31m[K53[m[K3.txt

NTFS 3.1 - Master File Table Denial of Service
| windows/dos/422[01;31m[K53[m[K.html

Nuke Evolution Xtreme 2.0 - Local File Inclusion / SQL Injection
| php/webapps/356[01;31m[K53[m[K.txt

Nuked-klaN 1.7.6 - Multiple Vulnerabilities
| php/webapps/[01;31m[K53[m[K39.php

Nvidia Stereoscopic 3D Driver Service 7.17.13.[01;31m[K53[m[K82 - Arbitrary Run Key Creation |
windows/local/38792.txt

O2PHP Oxygen 1.0/1.1 - 'post.php' SQL Injection
| php/webapps/27[01;31m[K53[m[K5.txt

```
Observium 0.16.7[01;31m[K53[m[K3 - (Authenticated) Arbitrary Command
Execution                                          |
php/webapps/39745.txt

Observium 0.16.7[01;31m[K53[m[K3 - Cross-Site Request Forgery
| php/webapps/39744.html

Ocean12 Membership Manager Pro - Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K54.txt

Octeth Oempro 3.6.4 - SQL Injection / Information Disclosure
| php/webapps/3[01;31m[K53[m[K11.txt

OfficeSIP Server 3.1 - Denial of Service
| windows/dos/184[01;31m[K53[m[K.txt

Okul Otomasyon Portal 2.0 - SQL Injection
| php/webapps/4[01;31m[K53[m[K9.txt

OLIB 7 WebView 2.5.1.1 - 'infile' Local File Inclusion
| php/webapps/66[01;31m[K53[m[K.txt

OmniHTTPd 1.1/2.0.x/2.4 - 'test.php' Sample Application Cross-Site
Scripting                                  |
windows/remote/217[01;31m[K53[m[K.txt

OneHTTPD 0.7 - Denial of Service
| windows/dos/275[01;31m[K53[m[K.py

OneWorldStore - IDOrder Information Disclosure
| asp/webapps/25[01;31m[K53[m[K0.txt

Online Grades & Attendance 3.2.6 - Multiple Local File Inclusions
| php/webapps/88[01;31m[K53[m[K.txt

Online Library Management System 1.0 - 'Search' SQL Injection
| php/webapps/500[01;31m[K53[m[K.txt

Online Quiz Maker 1.0 - 'catid' SQL Injection
| php/webapps/4[01;31m[K53[m[K23.txt

Online Work Order System (OWOS) Professional Edition - Authentication
Bypass                                     |
asp/webapps/1[01;31m[K53[m[K97.txt

Onlineon E-Ticaret - Database Disclosure
| asp/webapps/347[01;31m[K53[m[K.py

Open Auto Classifieds 1.4.3b - SQL Injection
| php/webapps/5[01;31m[K53[m[K1.txt

Open Auto Classifieds 1.5.9 - Multiple Vulnerabilities
| php/webapps/9[01;31m[K53[m[K0.txt
```

```
Open Conference Systems 1.1.4 - 'fullpath' File Inclusion
| php/webapps/2[01;31m[K53[m[K6.txt

Open-AudIT Community 2.1.1 - Cross-Site Scripting
| multiple/webapps/450[01;31m[K53[m[K.txt

OpenBB 1.0.x - 'myhome.php?to' Cross-Site Scripting
| php/webapps/240[01;31m[K53[m[K.txt

Opencart 1.1.8 - 'route' Local File Inclusion
| php/webapps/8[01;31m[K53[m[K9.txt

OpenCart 3.0.3.2 - Stored Cross Site Scripting (Authenticated)
| php/webapps/48[01;31m[K53[m[K9.txt

OpenElec 3.01 - 'obj' Local File Inclusion
| php/webapps/6[01;31m[K53[m[K0.txt

OpenNewsletter 2.5 - 'Compose.php' Cross-Site Scripting
| php/webapps/308[01;31m[K53[m[K.txt

OpenRat 0.8-beta4 - 'tpl_dir' Remote File Inclusion
| php/webapps/6[01;31m[K53[m[K8.txt

OpenSSH 1.2 - '.scp' File Create/Overwrite
| linux/remote/202[01;31m[K53[m[K.sh

Opera 7.10 - Permanent Denial of Service
| multiple/dos/22[01;31m[K53[m[K6.txt

Opera Web Browser 7.[01;31m[K53[m[K - Location Replace URI Obfuscation
| multiple/remote/24325.html

Opera Web Browser 8.0/8.5 - HTML Form Status Bar Misrepresentation
| multiple/remote/26[01;31m[K53[m[K1.html

Oracle 10g Database - 'SUBSCRIPTION_NAME' SQL Injection (2)
| multiple/remote/254[01;31m[K53[m[K.pl

Oracle 8.x/9.x/10.x Database - Multiple SQL Injections
| multiple/remote/2[01;31m[K53[m[K96.txt

Oracle 9i - Multiple Vulnerabilities
| unix/remote/243[01;31m[K53[m[K.sql

Oracle Database 10.1 - MDSYS.MD2.SDO_CODE_SIZE Buffer Overflow
| multiple/remote/2[01;31m[K53[m[K97.txt

Oracle Document Capture - Actbar2.ocx Insecure Method
| windows/remote/160[01;31m[K53[m[K.txt

Oracle Forms and Reports 11.1 - Arbitrary Code Execution
| jsp/remote/312[01;31m[K53[m[K.rb
```

Oracle Internet Directory 10.1.2.0.2 - 'oidldapd' Remote Memory Corruption |
multiple/dos/33[01;31m[K53[m[K2.txt

Oracle Java - Floating-Point Value Denial of Service
| multiple/dos/3[01;31m[K53[m[K04.txt

Oracle MySQL - 'ALTER DATABASE' Remote Denial of Service
| multiple/dos/14[01;31m[K53[m[K7.txt

Oracle Weblogic Server 10.3.6.0 / 12.1.3.0 / 12.2.1.2 / 12.2.1.3 - Deserialization Remote Command Executio |
multiple/remote/445[01;31m[K53[m[K.py

orangescrum 1.8.0 - 'Multiple' SQL Injection (Authenticated)
| multiple/webapps/505[01;31m[K53[m[K.txt

Orbis CMS 1.0.2 - 'editor-body.php' Cross-Site Scripting
| php/webapps/342[01;31m[K53[m[K.txt

Orchard CMS 1.7.3/1.8.2/1.9.0 - Persistent Cross-Site Scripting
| asp/webapps/37[01;31m[K53[m[K3.txt

osCommerce 2.2 - '/admin/reviews.php?page' Cross-Site Scripting
| php/webapps/287[01;31m[K53[m[K.txt

osTicket 1.11 - Cross-Site Scripting / Local File Inclusion
| php/webapps/467[01;31m[K53[m[K.txt

OTRS 5.0.x/6.0.x - Remote Command Execution (1)
| perl/webapps/438[01;31m[K53[m[K.txt

Ourgame GLWorld 2.x - 'hgs_startNotify()' ActiveX Buffer Overflow
| windows/remote/51[01;31m[K53[m[K.asp

Outlook for Android - Attachment Download Directory Traversal
| android/remote/433[01;31m[K53[m[K.py

OutSystems Service Studio 11.[01;31m[K53[m[K.30 - DLL Hijacking
| windows/local/51678.txt

Ovidentia 5.6.x/5.8 - 'statart.php?babInstallPath' Remote File Inclusion |
php/webapps/279[01;31m[K53[m[K.txt

OZJournals 2.1.1 - 'id' File Disclosure
| php/webapps/49[01;31m[K53[m[K.txt

paBugs 2.0 Beta 3 - 'main.php?cid' SQL Injection
| php/webapps/42[01;31m[K53[m[K.pl

PacketTrap Networks pt360 2.0.39 TFTPD - Remote Denial of Service
| windows/dos/[01;31m[K53[m[K16.py

```
PAD Site Scripts 3.6 - 'list.php?string' SQL Injection
| php/webapps/9[01;31m[K53[m[K1.txt

Panda ActiveScan 5.[01;31m[K53[m[K - 'Ascan_6.asp' ActiveX Control
Cross-Site Scripting                                  |
windows/remote/28373.txt

Pandora Fms - SQL Injection Remote Code Execution (Metasploit)
| php/remote/3[01;31m[K53[m[K80.rb

PaoBacheca 2.1 - 'index.php' URI Cross-Site Scripting
| php/webapps/344[01;31m[K53[m[K.txt

PC Tools Firewall Plus 7.0.0.123 - Local Denial of Service
| windows/dos/194[01;31m[K53[m[K.cpp

PDF Explorer 1.5.66.2 - Denial of Service (PoC)
| windows/dos/4[01;31m[K53[m[K89.py

PDF-XChange Viewer 2.5 Build 314.0 - Code Execution
| windows/local/42[01;31m[K53[m[K7.txt

PEEL Shopping 9.3.0 - 'address' Stored Cross-Site Scripting
| php/webapps/495[01;31m[K53[m[K.txt

PeopleAggregator 1.2pre6-release-[01;31m[K53[m[K - Multiple Remote File
Inclusions                                        | php/webapps/4551.txt

Persism CMS 0.9.2 - system[path] Remote File Inclusion
| php/webapps/38[01;31m[K53[m[K.txt

Pet Shop Management System 1.0 - Remote Code Execution (RCE)
(Unauthenticated)                                 |
php/webapps/503[01;31m[K53[m[K.php

pfSense 2.4.4-p1 (HAProxy Package 0.59_14) - Persistent Cross-Site
Scripting                                     |
php/webapps/46[01;31m[K53[m[K8.txt

PG eLms Pro vDEC_2007_01 - 'contact_us.php' Multiple POST Cross-Site
Scripting Vulnerabilities                |
php/webapps/17[01;31m[K53[m[K1.txt

PG eLms Pro vDEC_2007_01 - Multiple Blind SQL Injections
| php/webapps/17[01;31m[K53[m[K2.txt

Phaos 0.9.2 - 'basename()' Remote Command Execution
| php/webapps/22[01;31m[K53[m[K.php

Photo To Video Converter Professional 8.07 - Buffer Overflow (SEH)
| windows_x86/local/4[01;31m[K53[m[K[01;31m[K53[m[K.py
```

```
photo-rigma.biz 30 - SQL Injection / Cross-Site Scripting
| php/webapps/8[01;31m[K53[m[K2.txt

PhotoKorn 1.[01;31m[K53[m[K/1.54 - 'id' SQL Injection
| php/webapps/27732.txt

PhotoKorn 1.[01;31m[K53[m[K/1.54 - 'index.php' Multiple SQL
Injections                                                  |
php/webapps/27731.txt

PhotoKorn 1.[01;31m[K53[m[K/1.54 - 'print.php?cat' SQL Injection
| php/webapps/27733.txt

Photopad 1.2 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K53[m[K51.txt

PhotoPost PHP 4.6.5 - 'ecard.php' SQL Injection
| php/webapps/144[01;31m[K53[m[K.txt

PhotoPost Pro 5.1 - 'showgallery.php' Multiple Cross-Site Scripting
Vulnerabilities                          |
php/webapps/2[01;31m[K53[m[K08.txt

PhotoPost Pro 5.1 - 'showmembers.php' Multiple Cross-Site Scripting
Vulnerabilities                          |
php/webapps/2[01;31m[K53[m[K09.txt

PhotoPost Pro 5.1 - 'showmembers.php?sl' SQL Injection
| php/webapps/2[01;31m[K53[m[K11.txt

PhotoPost Pro 5.1 - 'showphoto.php?photo' SQL Injection
| php/webapps/2[01;31m[K53[m[K12.txt

PhotoPost Pro 5.1 - 'Slideshow.php?photo' Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K10.txt

PHP 5.2.5 - cURL 'safe_mode' Security Bypass
| php/remote/310[01;31m[K53[m[K.php

PHP 5.3.5 - 'grapheme_extract()' Null Pointer Dereference Denial of
Service                                  | php/dos/3[01;31m[K53[m[K54.txt

PHP 5.5.12 - Locale::parseLocale Memory Corruption
| php/dos/3[01;31m[K53[m[K58.txt

PHP 5.5.33 - Invalid Memory Write
| php/dos/396[01;31m[K53[m[K.txt

PHP 5.x COM - Safe Mode / disable_functions Bypass
| windows/local/45[01;31m[K53[m[K.php

PHP B2B Script 3.05 - SQL Injection
| php/webapps/41[01;31m[K53[m[K2.txt
```

```
PHP Content Architect 0.9 pre 1.2 - 'MFA_Theme.php' Remote File
Inclusion                                    |
php/webapps/299[01;31m[K53[m[K.txt

PHP Dashboards NEW 4.4 - Arbitrary File Read
| php/webapps/426[01;31m[K53[m[K.txt

PHP File Browser Script 1 - Directory Traversal
| php/webapps/4[01;31m[K53[m[K27.txt

PHP Jokesite 2.0 - 'joke_id' SQL Injection
| php/webapps/42[01;31m[K53[m[K4.txt

PHP Link Manager 1.7 - URL Redirection
| php/webapps/12[01;31m[K53[m[K4.txt

PHP Photo Gallery 1.0 - 'photo_id' SQL Injection
| php/webapps/[01;31m[K53[m[K64.txt

PHP Timeclock 1.04 - 'Multiple' Cross Site Scripting (XSS)
| php/webapps/498[01;31m[K53[m[K.txt

PHP-Charts 1.0 - 'index.php?type' Remote Code Execution
| php/webapps/264[01;31m[K53[m[K.py

PHP-FPM + Nginx - Remote Code Execution
| php/webapps/475[01;31m[K53[m[K.md

PHP-Fusion 4.0/5.0/6.0 - 'options.php?/ viewforum.php' SQL Injection
| php/webapps/26[01;31m[K53[m[K8.txt

PHP-Gastebuch 1.60 - Information Disclosure
| php/webapps/229[01;31m[K53[m[K.txt

PHP-Lance 1.52 - 'subcat' SQL Injection
| php/webapps/42[01;31m[K53[m[K3.txt

PHP-Nuke 6.x/7.x 'Downloads' Module - 'Lid' Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K41.html

PHP-Nuke 6.x/7.x Your_Account Module - 'Username' Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K39.txt

PHP-Nuke 6.x/7.x Your_Account Module - Avatarcategory Cross-Site
Scripting                                    |
php/webapps/2[01;31m[K53[m[K40.txt

PHP-Nuke 7.6 - 'banners.php' Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K43.txt

PHP-Nuke 7.6 Web_Links Module - Multiple Cross-Site Scripting
Vulnerabilities                              |
php/webapps/2[01;31m[K53[m[K42.txt
```

PHP-Nuke 7.6 Web_Links Module - Multiple SQL Injections
| php/webapps/2[01;31m[K53[m[K60.txt

PHP-Nuke 7.x - 'Block-Old_Articles.php' SQL Injection
| php/webapps/294[01;31m[K53[m[K.php

PHP-Nuke 8.3 - 'upload.php' Arbitrary File Upload (1)
| php/webapps/358[01;31m[K53[m[K.php

PHP-Nuke Nuke League Module - 'tid' Cross-Site Scripting
| php/webapps/32[01;31m[K53[m[K8.txt

PHP-revista 1.1.2 - Multiple SQL Injections
| php/webapps/3[01;31m[K53[m[K8.txt

PHP-Update 2.7 - 'extract()' Authentication Bypass / Shell Injection
| php/webapps/29[01;31m[K53[m[K.php

PHP/FI 1.0/FI 2.0/FI 2.0 b10 - mylog/mlog
| php/remote/195[01;31m[K53[m[K.txt

PHPAddressBook 2.0 - 'index.php' SQL Injection
| php/webapps/31[01;31m[K53[m[K9.txt

PHPads 213607 - Authentication Bypass / Password Change
| php/webapps/35[01;31m[K53[m[K5.php

phpBB 2.0.13 DLMan Pro Module - SQL Injection
| php/webapps/2[01;31m[K53[m[K44.txt

phpBB 2.0.13 Linkz Pro Module - SQL Injection
| php/webapps/2[01;31m[K53[m[K45.txt

phpBB Ajax Shoutbox 0.0.5 - Remote File Inclusion
| php/webapps/2[01;31m[K53[m[K2.txt

phpBB Import Tools Mod 0.1.4 - Remote File Inclusion
| php/webapps/2[01;31m[K53[m[K1.txt

phpBB Module XS-Mod 2.3.1 - Local File Inclusion
| php/webapps/[01;31m[K53[m[K01.txt

phpBB Photo Album 2.0.[01;31m[K53[m[K Module - 'Album_Cat.php' Cross-Site Scripting |
php/webapps/25403.txt

phpBB Photo Album Module 2.0.[01;31m[K53[m[K - 'Album_Comment.php' Cross-Site Scripting |
php/webapps/25404.txt

phpBB PJIRC Module 0.5 - 'irc.php' Local File Inclusion
| php/webapps/31[01;31m[K53[m[K5.txt

```
phpBB Plus 1.[01;31m[K53[m[K - 'phpbb_root_path' Remote File Inclusion
| php/webapps/4434.txt

phpBB PlusXL 2.0_272 - 'constants.php' Remote File Inclusion
| php/webapps/2[01;31m[K53[m[K8.pl

phpBB SpamBlocker Mod 1.0.2 - Remote File Inclusion
| php/webapps/2[01;31m[K53[m[K3.py

phpBB XS 0.58a - 'phpbb_root_path' Remote File Inclusion
| php/webapps/24[01;31m[K53[m[K.txt

PHPBB2 Plus 1.5 - 'GroupCP.php' Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K98.txt

PHPBB2 Plus 1.5 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                                  |
php/webapps/2[01;31m[K53[m[K99.txt

PHPBB2 Plus 1.[01;31m[K53[m[K - 'kb.php' SQL Injection
| php/webapps/33772.txt

phpBB2 Plus 1.[01;31m[K53[m[K - Acronym Mod SQL Injection
| php/webapps/3033.txt

PhpBlock a8.4 - 'PATH_TO_CODE' Remote File Inclusion
| php/webapps/[01;31m[K53[m[K48.txt

phpBP RC3 (2.204) - SQL Injection / Remote Code Execution
| php/webapps/31[01;31m[K53[m[K.php

Phpclanwebsite 1.23.1 - SQL Injection
| php/webapps/14[01;31m[K53[m[K.pl

phpCoin 1.2 - 'auxpage.php?page' Traversal Arbitrary File Access
| php/webapps/2[01;31m[K53[m[K02.txt

PHPcounter 1.3.2 - 'defs.php' Local File Inclusion
| php/webapps/65[01;31m[K53[m[K.txt

phpDirectorySource 1.1 - Multiple SQL Injections
| php/webapps/5[01;31m[K53[m[K7.txt

PHPGedView 4.1 - 'login.php' Cross-Site Scripting
| php/webapps/30[01;31m[K53[m[K4.txt

PHPJabbers Rental Property Booking 2.0 - Reflected XSS
| php/webapps/516[01;31m[K53[m[K.txt

PHPJabbers Vacation Packages Listing 2.0 - Multiple Vulnerabilities
| php/webapps/309[01;31m[K53[m[K.txt
```

```
PHPKit 1.6.1 R2 - 'overview.php' SQL Injection
| php/webapps/1[01;31m[K53[m[K50.rb

phpLiterAdmin 1.0 RC1 - Authentication Bypass
| php/webapps/1[01;31m[K53[m[K22.txt

phpMyAdmin 2.11.1 - 'setup.php' Cross-Site Scripting
| php/webapps/306[01;31m[K53[m[K.txt

phpMyAdmin 2.6 - 'display_tbl_links.lib.php' Multiple Cross-Site
Scripting Vulnerabilities                 |
php/webapps/251[01;31m[K53[m[K.txt

phpMyAdmin 2.x - Convcharset Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K30.txt

phpMyAdmin 3.0.1 - 'pmd_pdf.php' Cross-Site Scripting
| php/webapps/32[01;31m[K53[m[K1.txt

phpMyAdmin 4.0.x/4.1.x/4.2.x - Denial of Service
| php/dos/35[01;31m[K53[m[K9.txt

phpMyBackupPro 2.5 - Remote Command Execution / Cross-Site Request
Forgery                                   |
php/webapps/394[01;31m[K53[m[K.txt

phpMyBlockchecker 1.0.0055 - Insecure Cookie Handling
| php/webapps/90[01;31m[K53[m[K.txt

PHPMyConferences 8.0.2 - 'menu.inc.php' File Inclusion
| php/webapps/2[01;31m[K53[m[K5.txt

PHPMyRecipes 1.2.2 - 'dosearch.php?words_exact' SQL Injection
| php/webapps/3[01;31m[K53[m[K65.py

PHPMyRecipes 1.2.2 - 'viewrecipe.php?r_id' SQL Injection
| php/webapps/24[01;31m[K53[m[K7.txt

PHPMyVisites 1.3 - 'Set_Lang' File Inclusion
| php/webapps/25[01;31m[K53[m[K1.html

PHPMyWind 5.3 - Cross-Site Scripting
| php/webapps/42[01;31m[K53[m[K5.txt

phpProfiles - Multiple Vulnerabilities
| php/webapps/37[01;31m[K53[m[K7.txt

PHPSANE 0.5.0 - 'save.php' Remote File Inclusion
| php/webapps/9[01;31m[K53[m[K3.txt

phpscripte24 Countdown Standart Rückwärts Auktions System - SQL
Injection                                 |
php/webapps/12[01;31m[K53[m[K5.txt
```

```
phpShop 0.8.1 - 'page' Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K87.txt

PHPSpamManager 0.[01;31m[K53[m[Kb - 'body.php' Remote File Disclosure
| php/webapps/[01;31m[K53[m[K28.txt

PHPVID 0.9.9 - 'categories_type.php' SQL Injection
| php/webapps/41[01;31m[K53[m[K.txt

phpWebSite 0.9.3 - 'links.php' SQL Injection
| php/webapps/325[01;31m[K53[m[K.txt

PHPXref 0.7 - 'nav.html' Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K29.txt

PicaJet FX 2.6.5 - Denial of Service (PoC)
| windows_x86/dos/4[01;31m[K53[m[K83.py

Picture Rating 1.0 - Blind SQL Injection
| php/webapps/[01;31m[K53[m[K76.pl

PIGMy-SQL 1.4.1 - 'getdata.php' Blind SQL Injection
| php/webapps/[01;31m[K53[m[K67.pl

PilusCart 1.4.1 - Cross-Site Request Forgery (Add Admin)
| php/webapps/46[01;31m[K53[m[K1.html

Pinkie 2.15 - TFTP Remote Buffer Overflow (PoC)
| windows/dos/50[01;31m[K53[m[K5.py

Pinnacle Cart - 'index.php' Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K94.txt

PIPL 2.5.0 - '.m3u' Universal Buffer Overflow (SEH)
| windows/local/9[01;31m[K53[m[K6.py

Piwik Open Flash Chart - Remote Code Execution
| php/webapps/10[01;31m[K53[m[K2.txt

PixGPS 1.1.8 - Denial of Service (PoC)
| windows_x86/dos/4[01;31m[K53[m[K81.py

Platinum SDK Library - POST UPnP 'sscanf' Buffer Overflow (PoC)
| multiple/dos/1[01;31m[K53[m[K46.c

Plesk Small Business Manager 10.2.0 and Site Editor - Multiple
Vulnerabilities                                  |
php/webapps/1[01;31m[K53[m[K13.txt

Pluck CMS 4.5.3 - 'g_pcltar_lib_dir' Local File Inclusion
| php/webapps/71[01;31m[K53[m[K.txt
```

```
PluggedOut CMS 0.4.8 - 'contenttypeid' SQL Injection
| php/webapps/260[01;31m[K53[m[K.txt

PortWise SSL VPN 4.6 - 'reloadFrame' Cross-Site Scripting
| multiple/remote/336[01;31m[K53[m[K.txt

PostNuke Phoenix 0.760 RC3 - 'Module' Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K67.txt

PostNuke Phoenix 0.760 RC3 - 'OP' Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K66.txt

PostNuke Phoenix 0.760 RC3 - 'SID' SQL Injection
| php/webapps/2[01;31m[K53[m[K68.txt

Poultry Farm Management System v1.0 - Remote Code Execution (RCE)
| php/webapps/520[01;31m[K53[m[K.py

PowerBook 1.21 - 'index.php' Local File Inclusion
| php/webapps/[01;31m[K53[m[K02.txt

PowerDVD 5.0.1107 - 'trigger.dll' DLL Loading Arbitrary Code Execution
| windows/remote/348[01;31m[K53[m[K.c

PowerPHPBoard 1.00b - Multiple Local File Inclusions
| php/webapps/[01;31m[K53[m[K03.txt

PowerStrip 3.84 - 'pstrip.sys' Local Privilege Escalation
| windows/local/7[01;31m[K53[m[K3.txt

pppBlog 0.3.8 - System Disclosure
| php/webapps/18[01;31m[K53[m[K.php

Pragyan CMS 2.6.4 - Multiple SQL Injections
| php/webapps/8[01;31m[K53[m[K3.txt

Privacyware Privatefirewall 7.0 - Unquoted Service Path Privilege
Escalation                                |
windows/local/3[01;31m[K53[m[K22.txt

Professional Download Assistant 0.1 - SQL Injection
| asp/webapps/326[01;31m[K53[m[K.txt

ProfitCode Software PayProCart 3.0 - 'Usrdetails.php' Cross-Site
Scripting                                  |
php/webapps/2[01;31m[K53[m[K37.txt

profitcode software payprocart 3.0 - Directory Traversal
| php/webapps/2[01;31m[K53[m[K38.txt

ProFTPd 1.2 - 'SIZE' Remote Denial of Service
| linux/dos/20[01;31m[K53[m[K6.java
```

Program Checker - 'sasatl.dll 1.5.0.[01;31m[K53[m[K1' DebugMsgLog HeapSpray | windows/remote/4177.html

Program Checker - 'sasatl.dll 1.5.0.[01;31m[K53[m[K1' JavaScript HeapSpray | windows/remote/4170.html

Proxifier for Mac 2.18 - Multiple Vulnerabilities | macos/local/418[01;31m[K53[m[K.txt

Prozilla Cheat Script 2.0 - 'id' SQL Injection | php/webapps/[01;31m[K53[m[K89.txt

Prozilla Forum Service - 'forum' SQL Injection | php/webapps/[01;31m[K53[m[K85.txt

Prozilla Freelancers - 'project' SQL Injection | php/webapps/[01;31m[K53[m[K90.txt

Prozilla Reviews Script 1.0 - Arbitrary Delete User | php/webapps/[01;31m[K53[m[K87.txt

Prozilla Top 100 1.2 - Arbitrary Delete Stats | php/webapps/[01;31m[K53[m[K84.txt

Prozilla Topsites 1.0 - Arbitrary Edit/Add Users | php/webapps/[01;31m[K53[m[K88.txt

Pub-Me CMS - Blind SQL Injection | php/webapps/1[01;31m[K53[m[K48.txt

Pulse Pro 1.4.3 - Persistent Cross-Site Scripting | php/webapps/1[01;31m[K53[m[K08.txt

PuterJam's Blog PJBlog3 3.0.6 - 'action.asp' SQL Injection | asp/webapps/329[01;31m[K53[m[K.vbs

PuTTy.exe 0.[01;31m[K53[m[K - Remote Buffer Overflow (Metasploit) | windows/remote/16463.rb

PuTTy.exe 0.[01;31m[K53[m[K - Validation Remote Buffer Overflow (Metasploit) | windows/remote/1788.pm

PwsPHP 1.2.3 - 'index.php' SQL Injection | php/webapps/1[01;31m[K53[m[K2.pl

PyLoad 0.5.0 - Pre-auth Remote Code Execution (RCE) | python/webapps/51[01;31m[K53[m[K2.py

Python 2.5.2 - 'Imageop' Module Argument Validation Buffer Overflow | unix/dos/32[01;31m[K53[m[K4.py

PZ Frontend Manager WordPress Plugin 1.0.5 - Cross Site Request Forgery (CSRF) | php/webapps/521[01;31m[K53[m[K.NA

QEMU - Floppy Disk Controller (FDC) (PoC) | multiple/dos/370[01;31m[K53[m[K.c

QNAP Photo Station 5.7.0 - Cross-Site Scripting | hardware/webapps/4[01;31m[K53[m[K48.txt

QNAP QTS and Photo Station 6.0.3 - Remote Command Execution | php/webapps/48[01;31m[K53[m[K1.py

QNX 6.4.x/6.5.x ifwatchd - Local Privilege Escalation | qnx/local/321[01;31m[K53[m[K.sh

Qualcomm qpopper 2.[01;31m[K53[m[K/3.0 / RedHat imap 4.5 -4 / UoW imap 4.5 popd - Lock File Denial of Service | linux/dos/19869.txt

Qualcomm WorldMail Server 3.0 - Directory Traversal | linux/remote/26[01;31m[K53[m[K6.txt

Quali CloudShell 7.1.0.6508 (Patch 6) - Persistent Cross-Site Scripting | windows/webapps/424[01;31m[K53[m[K.txt

QuestCMS - Cross-Site Scripting / Directory Traversal / SQL Injection | php/webapps/68[01;31m[K53[m[K.txt

Quick 'n Easy FTP Server Lite 3.1 - Denial of Service | windows/dos/128[01;31m[K53[m[K.py

Quick TFTP Server Pro 2.1 - Remote Overflow (SEH) | windows/remote/[01;31m[K53[m[K15.py

Quick.CMS 6.7 - Cross Site Request Forgery (CSRF) to Cross Site Scripting (XSS) (Authenticated) | php/webapps/50[01;31m[K53[m[K0.txt

QuickBox Pro 2.1.8 - Authenticated Remote Code Execution | php/webapps/48[01;31m[K53[m[K6.py

Quickzip 5.1.8.1 - Denial of Service | windows/dos/1[01;31m[K53[m[K93.pl

Racer 0.5.3 Beta 5 - Remote Stack Buffer Overflow | windows/remote/82[01;31m[K53[m[K.c

RadScripts RadBids Gold 2.0 - 'faq.php?farea' Cross-Site Scripting | php/webapps/2[01;31m[K53[m[K71.txt

RadScripts RadBids Gold 2.0 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/2[01;31m[K53[m[K72.txt

RadScripts RadBids Gold 2.0 - 'index.php?mode' SQL Injection
| php/webapps/2[01;31m[K53[m[K70.txt

RadScripts RadBids Gold 2.0 - 'index.php?read' Traversal Arbitrary File
Access | php/webapps/2[01;31m[K53[m[K69.txt

RarmaRadio 2.[01;31m[K53[m[K.1 - '.m3u' Denial of Service
| windows/dos/1[01;31m[K53[m[K05.pl

Real Player - 'rmoc3260.dll' ActiveX Control Remote Code Execution
| windows/remote/[01;31m[K53[m[K32.html

Real Player v.20.0.8.310 G2 Control - 'DoGoToURL()' Remote Code
Execution (RCE) |
windows/local/509[01;31m[K53[m[K.txt

Realtek Audio Control Panel 1.0.1.65 - Local Buffer Overflow
| windows/local/15[01;31m[K53[m[K9.pl

Redaction System 1.0 - 'lang_prefix' Remote File Inclusion
| php/webapps/2[01;31m[K53[m[K4.pl

RedCMS 0.1 - 'login.php' Multiple SQL Injections
| php/webapps/27[01;31m[K53[m[K9.txt

RedCMS 0.1 - 'profile.php?u' SQL Injection
| php/webapps/27[01;31m[K53[m[K8.txt

ReiserFS 3.5.28 (Linux Kernel) - Code Execution / Denial of Service
| linux/dos/20[01;31m[K53[m[K5.txt

Responsive Matrimonial Script 4.0.1 - SQL Injection
| php/webapps/41[01;31m[K53[m[K3.txt

Resumes Management and Job Application Website 1.0 - Authentication
Bypass |
php/webapps/493[01;31m[K53[m[K.txt

Revize CMS - 'Query_results.jsp' SQL Injection
| jsp/webapps/26[01;31m[K53[m[K2.txt

Revize CMS - 'Revize.XML' Information Disclosure
| jsp/webapps/26[01;31m[K53[m[K3.txt

Revize CMS HTTPTranslatorServlet - Cross-Site Scripting
| jsp/webapps/26[01;31m[K53[m[K4.txt

ReVou Twitter Clone - Arbitrary File Upload
| php/webapps/7[01;31m[K53[m[K1.txt

Richard Gooch SimpleInit 2.0.2 - Open File Descriptor
| linux/local/21[01;31m[K53[m[K8.c

```
RIPS 0.[01;31m[K53[m[K - Multiple Local File Inclusions
| php/webapps/18660.txt

Rising - 'RSNTGDI.sys' Local Denial of Service
| windows/dos/1[01;31m[K53[m[K83.c

Rit Research Labs The Bat! 1.[01;31m[K53[m[K - Microsoft Denial of
Service Device Name Denial of Service                |
windows/dos/21307.txt

Rivettracker 1.03 - Multiple SQL Injections
| multiple/webapps/185[01;31m[K53[m[K.txt

RM Downloader 3.0.2.1 - '.asx' Local Buffer Overflow (SEH)
| windows/local/119[01;31m[K53[m[K.py

RoboImport 1.2.0.72 - Denial of Service (PoC)
| windows_x86/dos/4[01;31m[K53[m[K82.py

RobotStats 1.0 - 'robot' SQL Injection
| php/webapps/3[01;31m[K53[m[K44.txt

RobotStats 1.0 - HTML Injection
| aix/dos/3[01;31m[K53[m[K42.txt

Rock Band CMS 0.10 - 'news.php' Multiple SQL Injections (1)
| php/webapps/95[01;31m[K53[m[K.txt

Rocket.Chat 2.1.0 - Cross-Site Scripting
| linux/webapps/47[01;31m[K53[m[K7.txt

RoSPORA 1.5.0 - Remote PHP Code Injection
| php/webapps/1[01;31m[K53[m[K43.php

Roundcube Webmail 0.2b - Remote Code Execution
| php/webapps/75[01;31m[K53[m[K.sh

RPi Cam Control < 6.4.25 - 'preview.php' Remote Command Execution
| linux/webapps/4[01;31m[K53[m[K61.py

RTTucson Quotations Database Script - Authentication Bypass
| php/webapps/24[01;31m[K53[m[K3.txt

Rubedo CMS 3.4.0 - Directory Traversal
| linux/webapps/4[01;31m[K53[m[K85.txt

Ruby on Rails 3.0.5 - 'WEBrick::HTTPRequest' Module HTTP Header
Injection                                    |
multiple/remote/3[01;31m[K53[m[K52.rb

RUMBA 7.3/7.4 - Profile Handling Multiple Buffer Overflow
Vulnerabilities                                      |
windows/dos/2[01;31m[K53[m[K26.txt
```

```
Rumba XM - Cross-Site Scripting
| php/webapps/10[01;31m[K53[m[K4.txt

Rumble Mail Server 0.51.3135 - 'servername' Stored XSS
| multiple/webapps/492[01;31m[K53[m[K.txt

RunCMS 2.2.2 - 'register.php' SQL Injection
| php/webapps/3[01;31m[K53[m[K34.txt

RunCMS Module bamagalerie3 - SQL Injection
| php/webapps/[01;31m[K53[m[K40.txt

S.u.S.E Linux 4.x/5.x/6.x/7.0 / Slackware 3.x/4.0 / Turbolinux 6 /
OpenLinux 7.0 - 'fdmount' Local Buffer  |
linux/local/199[01;31m[K53[m[K.c

Sabros.us 1.75 - 'thumbnails.php' Remote File Disclosure
| php/webapps/[01;31m[K53[m[K60.txt

Sagem F@ST Routers - DHCP Hostname Cross-Site Request Forgery
| hardware/remote/6[01;31m[K53[m[K2.py

Sagem FAST3304-V2 - Authentication Bypass (2)
| hardware/webapps/385[01;31m[K53[m[K.txt

Salim Gasmi GLD (Greylisting Daemon) 1.x - Postfix Greylisting Daemon
Buffer Overflow                      |
linux/remote/2[01;31m[K53[m[K92.c

Samba 3.3.5 - Format String / Security Bypass
| linux/remote/330[01;31m[K53[m[K.txt

Samsung DVR Firmware 1.10 - Authentication Bypass
| hardware/webapps/277[01;31m[K53[m[K.txt

SAP Database 7.3/7.4 - SDBINST Race Condition
| linux/local/22[01;31m[K53[m[K1.pl

SAP NetWeaver - 7.[01;31m[K53[m[K - HTTP Request Smuggling
| multiple/remote/52109.txt

SAP NetWeaver Dispatcher - Multiple Vulnerabilities
| windows/dos/188[01;31m[K53[m[K.txt

saPHP Lesson 2.0 - 'forumid' SQL Injection
| php/webapps/1[01;31m[K53[m[K0.pl

Savsoft Quiz 5 - Stored Cross-Site Scripting
| php/webapps/487[01;31m[K53[m[K.txt

Schoolhos CMS 2.29 - Remote Code Execution / SQL Injection
| php/webapps/407[01;31m[K53[m[K.php
```

```
Schools Alert Management Script 2.01 - 'list_id' SQL Injection
| php/webapps/41[01;31m[K53[m[K4.txt

SCO OpenServer 5.0.6/5.0.7 - NWPrint Command Line Argument Local Buffer
Overflow                          | unix/local/2[01;31m[K53[m[K33.c

SCO Unixware 7.1.3 - 'ptrace' Local Privilege Escalation
| sco/local/1[01;31m[K53[m[K4.c

SCO UnixWare < 7.1.4 p[01;31m[K53[m[K4589 - 'pkgadd' Local Privilege
Escalation                                          |
sco/local/[01;31m[K53[m[K55.sh

SCO UnixWare Merge - 'mcd' Local Privilege Escalation
| sco/local/[01;31m[K53[m[K57.c

SCO UnixWare Reliant HA 1.1.4 - Local Privilege Escalation
| sco/local/[01;31m[K53[m[K56.c

ScorpNews 1.0 - 'site' Remote File Inclusion
| php/webapps/5[01;31m[K53[m[K9.txt

ScreenOS 1.73/2.x - Firewall Denial of Service
| sco/dos/20[01;31m[K53[m[K2.txt

ScriptCase 8.1.0[01;31m[K53[m[K - Multiple Vulnerabilities
| php/webapps/40791.txt

SDP Downloader 2.3.0 - '.asx' Local Buffer Overflow (SEH) (1)
| windows/local/8[01;31m[K53[m[K6.py

SDP Downloader 2.3.0 - '.asx' Local Heap Overflow (PoC)
| windows/dos/8[01;31m[K53[m[K1.pl

Seanox DevWex Windows Binary 1.2002.520 - File Disclosure
| windows/remote/21[01;31m[K53[m[K0.txt

Selea CarPlateServer (CPS) 4.0.1.6 - Local Privilege Escalation
| windows/local/494[01;31m[K53[m[K.txt

Select Your College Script 2.01 - SQL Injection
| php/webapps/41[01;31m[K53[m[K5.txt

SGI IRIX 6.4 - 'suid_exec' Local Privilege Escalation
| irix/local/193[01;31m[K53[m[K.txt

SGI IRIX 6.5.22 - GR_OSView Information Disclosure
| irix/local/2[01;31m[K53[m[K61.txt

SGI IRIX 6.5.22 - GR_OSView Local Arbitrary File Overwrite
| irix/local/2[01;31m[K53[m[K62.txt
```

Shopy Point of Sale 1.0 - CSV Injection
| php/webapps/44[01;31m[K53[m[K4.txt

SiliSoftware PHPThumb() 1.7.11-201108081[01;31m[K53[m[K7 -
'/demo/PHPThumb.demo.random.php?dir' Cross-Site Scripting |
php/webapps/37207.txt

SiliSoftware PHPThumb() 1.7.11-201108081[01;31m[K53[m[K7 -
'/demo/PHPThumb.demo.showpic.php?title' Cross-Site Scripting |
php/webapps/37206.txt

Silurus Classifieds System - 'category.php' SQL Injection
| php/webapps/9[01;31m[K53[m[K8.txt

Simple Forum PHP 2.4 - Cross-Site Request Forgery (Edit Options)
| php/webapps/40[01;31m[K53[m[K2.html

Simple Forum PHP 2.4 - SQL Injection
| php/webapps/40[01;31m[K53[m[K1.txt

Simple POS 4.0.24 - 'columns[0][search][value]' SQL Injection
| php/webapps/4[01;31m[K53[m[K28.txt

SimpleBlog 2.3 - '/admin/edit.asp' SQL Injection
| asp/webapps/28[01;31m[K53[m[K.txt

Simpli Easy (AFC Simple) NewsLetter 4.2 - Cross-Site Scripting /
Information Leakage |
php/webapps/1[01;31m[K53[m[K55.txt

Site Sift Listings - 'id' SQL Injection
| php/webapps/[01;31m[K53[m[K83.txt

Site2Nite Business eListings - SQL Injection
| asp/webapps/1[01;31m[K53[m[K99.txt

Site2Ntite Vacation Rental (VRBO) Listings - SQL Injection
| asp/webapps/1[01;31m[K53[m[K95.txt

SiteEnable - SQL Injection
| asp/webapps/2[01;31m[K53[m[K32.txt

Siteman 1.1 - User Database Privilege Escalation (2)
| php/webapps/250[01;31m[K53[m[K.html

SiteSearch Indexer 3.5 - 'searchresults.asp' Cross-Site Scripting
| asp/webapps/27[01;31m[K53[m[K6.txt

SitioOnline - SQL Injection
| php/webapps/104[01;31m[K53[m[K.txt

Skype Empresarial Office 365 16.0.10730.200[01;31m[K53[m[K - 'Dirección de inicio de sesión' Denial of service (PoC) | windows_x86-64/dos/45295.py

Smadav Anti Virus 9.1 - Crash (PoC)
| windows/dos/226[01;31m[K53[m[K.py

SmallFTPd 1.0.3 - Directory Traversal
| windows/remote/1[01;31m[K53[m[K58.txt

Smart Office Web 20.28 - Remote Information Disclosure (Unauthenticated) |
aspx/webapps/51[01;31m[K53[m[K9.py

SmartBlog 1.3 - 'index.php' SQL Injection
| php/webapps/5[01;31m[K53[m[K5.txt

Smarty Template Engine 2.6.9 - '$smarty.template' PHP Code Injection
| php/webapps/3[01;31m[K53[m[K43.txt

SMC Networks SMCD3G Session Management - Authentication Bypass
| multiple/remote/3[01;31m[K53[m[K16.sh

Smoothflash - 'cid' SQL Injection
| php/webapps/[01;31m[K53[m[K22.txt

snif 1.5.2 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/304[01;31m[K53[m[K.txt

snipe Gallery Script - SQL Injection
| php/webapps/140[01;31m[K53[m[K.txt

Snircd 1.3.4 - 'send_user_mode' Denial of Service
| multiple/dos/[01;31m[K53[m[K06.txt

SnowFlake CMS 0.9.5 Beta - 'uid' SQL Injection
| php/webapps/343[01;31m[K53[m[K.txt

Snowfox CMS 1.0 - Cross-Site Request Forgery (Add Admin)
| php/webapps/3[01;31m[K53[m[K01.html

Social Network Script 3.01 - 'id' SQL Injection
| php/webapps/41[01;31m[K53[m[K6.txt

Socusoft 3GP Photo Slideshow 8.05 - Buffer Overflow (SEH)
| windows_x86/local/4[01;31m[K53[m[K52.py

SocuSoft iPod Photo Slideshow 8.05 - Buffer Overflow (SEH)
| windows_x86/local/4[01;31m[K53[m[K50.py

Socusoft Photo 2 Video 8.05 - Local Buffer Overflow
| windows/local/18[01;31m[K53[m[K3.txt

```
Sofi WebGui 0.6.3 PRE - 'mod_dir' Remote File Inclusion
| php/webapps/6[01;31m[K53[m[K9.txt

Softneta MedDream PACS Server Premium 6.7.1.1 - Directory Traversal
| php/webapps/4[01;31m[K53[m[K47.txt

Software Index 1.1 - 'cid' SQL Injection
| php/webapps/[01;31m[K53[m[K78.txt

SolarCMS 0.[01;31m[K53[m[K.8 - 'Forum' Remote Cookies Disclosure
| php/webapps/7548.php

Solaris 7.0 - 'ufsdump' Local Buffer Overflow (1)
| solaris/local/19[01;31m[K53[m[K3.c

Solaris 7.0 - 'ufsdump' Local Buffer Overflow (2)
| solaris/local/19[01;31m[K53[m[K4.c

Soldier of Fortune II 1.3 Server/Client - Denial of Service
| windows/dos/6[01;31m[K53[m[K.c

Sonatype Nexus Repository 3.[01;31m[K53[m[K.0-01 - Path Traversal
| multiple/webapps/52101.py

SonicWALL AntiSpam & EMail 7.3.1 - Multiple Vulnerabilities
| multiple/remote/36[01;31m[K53[m[K7.txt

SonicWALL SOHO 5.1.7 - Web Interface Multiple Remote Input Validation
Vulnerabilities                        |
cgi/webapps/2[01;31m[K53[m[K31.txt

SonicWALL SOHO3 6.3 - Content Blocking Script Injection
| multiple/remote/214[01;31m[K53[m[K.txt

specview 2.5 build 8[01;31m[K53[m[K - Directory Traversal
| windows/webapps/19455.txt

Spider Player 2.4.5 - Denial of Service
| windows/dos/1[01;31m[K53[m[K02.py

SPIP v4.2.0 - Remote Code Execution (Unauthenticated)
| php/webapps/51[01;31m[K53[m[K6.py

Splunk 4.3.3 - Arbitrary File Read
| multiple/webapps/210[01;31m[K53[m[K.txt

SpoonLabs Vivvo Article Management CMS 3.40 - 'Show_Webfeed.php' SQL
Injection                              |
php/webapps/29[01;31m[K53[m[K4.txt

Squash - YAML Code Execution (Metasploit)
| multiple/remote/27[01;31m[K53[m[K0.rb
```

```
Squirrelcart PRO 3.0.0 - Blind SQL Injection
| php/webapps/1[01;31m[K53[m[K00.txt

SqWebMail 3.x/4.0 - HTTP Response Splitting
| php/webapps/25[01;31m[K53[m[K4.txt

SSC DiskAccess NFS Client - 'DAPCNFSD.dll' Remote Stack Buffer Overflow
| windows/remote/29[01;31m[K53[m[K8.c

Star Wars Jedi Knight: Jedi Academy 1.0.11 - Buffer Overflow (PoC)
| windows/dos/2[01;31m[K53[m[K29.cfg

study planner (studiewijzer) 0.15 - Remote File Inclusion
| php/webapps/3[01;31m[K53[m[K2.txt

Subrion CMS 4.0.5 - Cross-Site Request Forgery Bypass / Persistent
Cross-Site Scripting                    |
php/webapps/405[01;31m[K53[m[K.txt

Subversion 0.3.7/1.0.0 - Remote Buffer Overflow
| linux/remote/4[01;31m[K53[m[K7.c

SuiteCRM 7.11.18 - Remote Code Execution (RCE) (Authenticated)
(Metasploit)                                  |
php/webapps/50[01;31m[K53[m[K1.rb

Sun Java System Web Server 6.1/7.0 - Digest Authentication Remote
Buffer Overflow                           |
multiple/remote/335[01;31m[K53[m[K.txt

Sun JavaMail 1.3.2 - 'MimeBodyPart.getFileName' Directory Traversal
| multiple/remote/2[01;31m[K53[m[K95.txt

Sun Solaris 10 - rpc.ypupdated Remote Code Execution (Metasploit)
| solaris/remote/[01;31m[K53[m[K66.rb

SunFTP 1.0 Build 9 - Unauthorized File Access
| windows/remote/206[01;31m[K53[m[K.txt

SunLight CMS 5.3 - 'root' Remote File Inclusion
| php/webapps/39[01;31m[K53[m[K.txt

Super Socializer 7.13.52 - Reflected XSS
| php/webapps/51[01;31m[K53[m[K4.py

SupportPRO SupportDesk 3.0 - 'shownews.php' Cross-Site Scripting
| php/webapps/331[01;31m[K53[m[K.txt

Sybase Advantage Data Architect - '.SQL' Format Heap Overflow
| windows/dos/1[01;31m[K53[m[K78.py

Symantec ConsoleUtilities - ActiveX Buffer Overflow (Metasploit)
| windows/remote/98[01;31m[K53[m[K.rb
```

```
Symantec Endpoint Protection Manager 11.0/12.0/12.1 - Remote Command
Execution                                |
windows/remote/318[01;31m[K53[m[K.py

Symantec Mobile Encryption for iPhone 2.1.0 - 'Server' Denial of
Service (PoC)                             |
ios/dos/4[01;31m[K53[m[K18.py

Symantec SiteMinder WebAgent v12.52 - Cross-site scripting (XSS)
| hardware/webapps/51[01;31m[K53[m[K0.txt

SynaMan 4.0 build 1488 - (Authenticated) Cross-Site Scripting
| windows/webapps/4[01;31m[K53[m[K86.txt

SynaMan 4.0 build 1488 - SMTP Credential Disclosure
| windows/webapps/4[01;31m[K53[m[K87.txt

Sync Breeze Enterprise 10.1.16 - Denial of Service
| windows/dos/434[01;31m[K53[m[K.py

SynTail 1.5 Build 566 - Multiple Vulnerabilities
| php/webapps/369[01;31m[K53[m[K.txt

Sysax 5.[01;31m[K53[m[K - SSH 'Username' Remote Buffer Overflow
(Metasploit)                                          |
windows/remote/18557.rb

Sysax 5.[01;31m[K53[m[K - SSH 'Username' Remote Buffer Overflow Remote
Code Execution (Egghunter)                      |
windows/remote/18[01;31m[K53[m[K5.py

Sysax Multi Server 5.[01;31m[K53[m[K - SFTP (Authenticated) (SEH)
| windows/remote/18[01;31m[K53[m[K4.py

SystemTap 1.0 - 'stat-server' Arbitrary Command Injection
| linux/remote/33[01;31m[K53[m[K5.txt

Tandis CMS 2.5 - 'index.php' Multiple SQL Injections
| php/webapps/32[01;31m[K53[m[K3.txt

TaskFreak! 0.6.4 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                             |
php/webapps/3[01;31m[K53[m[K36.txt

TaskFreak! 0.6.4 - 'print_list.php' Multiple Cross-Site Scripting
Vulnerabilities                          |
php/webapps/3[01;31m[K53[m[K37.txt

TaskFreak! 0.6.4 - 'rss.php' HTTP Referer Header Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K38.txt

TCExam 11.1.16 - 'user_password' Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K06.txt
```

TCMS - Multiple Input Validation Vulnerabilities
| php/webapps/34[01;31m[K53[m[K4.txt

tcpdump 4.6.2 - Geonet Decoder Denial of Service
| multiple/dos/3[01;31m[K53[m[K59.txt

TDM Digital Signage PC Player 4.1 - Insecure File Permissions
| windows/local/489[01;31m[K53[m[K.txt

teamshare teamtrack 3.0 - Directory Traversal
| windows/remote/19[01;31m[K53[m[K7.txt

Tecnovision DLX Spot - SSH Backdoor Access
| multiple/remote/427[01;31m[K53[m[K.txt

Telekorn Signkorn Guestbook 1.x - '/admin/index.php?dir_path' Remote File Inclusion | php/webapps/28[01;31m[K53[m[K9.txt

Telekorn Signkorn Guestbook 1.x - '/admin/log.php?dir_path' Remote File Inclusion | php/webapps/28[01;31m[K53[m[K8.txt

Telekorn Signkorn Guestbook 1.x - '/admin/preview.php?dir_path' Remote File Inclusion | php/webapps/28[01;31m[K53[m[K7.txt

Telekorn Signkorn Guestbook 1.x - '/help/de/adminhelp0.php?dir_path' Remote File Inclusion | php/webapps/28[01;31m[K53[m[K2.txt

Telekorn Signkorn Guestbook 1.x - '/help/de/adminhelp1.php?dir_path' Remote File Inclusion | php/webapps/28[01;31m[K53[m[K3.txt

Telekorn Signkorn Guestbook 1.x - '/help/de/adminhelp2.php?dir_path' Remote File Inclusion | php/webapps/28[01;31m[K53[m[K4.txt

Telekorn Signkorn Guestbook 1.x - '/help/de/adminhelp3.php?dir_path' Remote File Inclusion | php/webapps/28[01;31m[K53[m[K5.txt

Telekorn Signkorn Guestbook 1.x - '/help/en/adminhelp2.php?dir_path' Remote File Inclusion | php/webapps/28[01;31m[K53[m[K0.txt

Telekorn Signkorn Guestbook 1.x - '/help/en/adminhelp3.php?dir_path' Remote File Inclusion | php/webapps/28[01;31m[K53[m[K1.txt

Telekorn Signkorn Guestbook 1.x - 'entry.php?dir_path' Remote File Inclusion | php/webapps/28[01;31m[K53[m[K6.txt

```
Telestream Flip4Mac - 'WMV' File Remote Memory Corruption
| osx/dos/29[01;31m[K53[m[K5.txt

Tenable WAS-Scanner 7.4.1708 - Remote Command Execution
| linux/remote/4[01;31m[K53[m[K45.txt

Tenda AC15 Router - Remote Code Execution
| hardware/remote/442[01;31m[K53[m[K.py

Tenda ADSL Router D152 - Cross-Site Scripting
| hardware/webapps/4[01;31m[K53[m[K36.txt

Tenda N11 Wireless Router 5.07.43_en_NEX01 - Remote DNS Change
| hardware/webapps/443[01;31m[K53[m[K.sh

Teraway LinkTracker 1.0 - Remote Password Change
| php/webapps/85[01;31m[K53[m[K.html

Termite 3.4 - Denial of Service (PoC)
| windows_x86/dos/454[01;31m[K53[m[K.py

TestLink 1.8.5 - 'order_by_login_dir' Cross-Site Scripting
| php/webapps/33[01;31m[K53[m[K4.txt

TFTgallery 0.13.1 - Local File Inclusion
| php/webapps/1[01;31m[K53[m[K45.txt

TFTP Server 1.4 - ST Buffer Overflow
| windows/remote/[01;31m[K53[m[K14.py

TFTPGUI 1.4.5 - Long Transport Mode Overflow Denial of Service
(Metasploit)                                  |
windows/dos/12[01;31m[K53[m[K0.rb

The Includer 1.0/1.1 - Remote File Inclusion
| php/webapps/2[01;31m[K53[m[K14.txt

ThisIsWhyImBroke Clone Script 4.0 - 'id' SQL Injection
| php/webapps/412[01;31m[K53[m[K.txt

Thomson SpeedTouch 2030 - SIP Empty Message Remote Denial of Service
| hardware/dos/30[01;31m[K53[m[K8.pl

Thomson SpeedTouch ST 2030 (SIP Phone) - SIP Invite Message Remote
Denial of Service                          |
hardware/dos/30[01;31m[K53[m[K0.pl

Tiki Wiki 15.1 - File Upload
| php/webapps/400[01;31m[K53[m[K.py

TikiWiki 2.2/3.0 - 'tiki-list_file_gallery.php' Cross-Site Scripting
| php/webapps/328[01;31m[K53[m[K.txt
```

TikiWiki Project 1.8 - 'messu-mailbox.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/239[01;31m[K53[m[K.txt

Tinypug 0.9.5 - Cross-Site Request Forgery (Password Change) | php/webapps/115[01;31m[K53[m[K.txt

Titan FTP Server 6.26 build 630 - Remote Denial of Service | windows/dos/67[01;31m[K53[m[K.py

TitanNit Web Control 2.01 / Atemio 7600 - Root Remote Code Execution | hardware/remote/518[01;31m[K53[m[K.py

Toms Gästebuch 1.00 - 'form.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/305[01;31m[K53[m[K.txt

TopperMod 1.0 - 'mod.php' Local File Inclusion | php/webapps/[01;31m[K53[m[K12.txt

TopperMod 2.0 - SQL Injection | php/webapps/[01;31m[K53[m[K11.txt

Total.js CMS 12 - Widget JavaScript Code Injection (Metasploit) | multiple/remote/47[01;31m[K53[m[K1.rb

TotalCalendar 2.30 - 'inc' Remote File Inclusion | php/webapps/17[01;31m[K53[m[K.txt

Touchpad / Trivum WebTouch Setup 2.[01;31m[K53[m[K build 13163 - Authentication Bypass | hardware/webapps/45063.txt

TP-Link TL-WR740N - Denial of Service | hardware/dos/3[01;31m[K53[m[K45.txt

Trend Micro OfficeScan - Client ActiveX Control Buffer Overflow (Metasploit) | windows/remote/16[01;31m[K53[m[K5.rb

Trend Micro OfficeScan Client 10.0 - ACL Service LPE | windows/local/514[01;31m[K53[m[K.txt

Trend Micro Titanium Maximum Security 2011 - Local Kernel | windows/local/1[01;31m[K53[m[K76.c

Trend Micro Virtual Mobile Infrastructure 5.5.1336 - 'Server address' Denial of Service (PoC) | ios/dos/4[01;31m[K53[m[K21.py

TRENDnet SecurView Wireless Network Camera TV-IP422WN - 'UltraCamX.ocx' Stack Buffer Overflow (PoC) | windows/dos/3[01;31m[K53[m[K63.txt

```
Trillian 6.1 Build 16 - 'Sign In' Denial of service (PoC)
| windows_x86-64/dos/4[01;31m[K53[m[K01.py

Truegalerie 1.0 - Unauthorized Administrative Access
| php/webapps/22[01;31m[K53[m[K4.txt

ttplayer 5.6Beta3 - Denial of Service (PoC)
| windows/dos/110[01;31m[K53[m[K.py

Tuleap Project Wiki 8.3 < 9.6.99.86 - Command Injection
| php/webapps/419[01;31m[K53[m[K.md

Tumbleweed SecureTransport 4.6.1 FileTransfer - ActiveX Buffer Overflow
| windows/remote/[01;31m[K53[m[K98.html

Tux CMS 0.1 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/317[01;31m[K53[m[K.txt

UApplication Ublog 1.0.x - Cross-Site Scripting
| php/webapps/2[01;31m[K53[m[K17.txt

Ubiquiti airOS - Arbitrary File Upload (Metasploit)
| unix/remote/398[01;31m[K53[m[K.rb

Uiga Church Portal - 'year' SQL Injection
| php/webapps/9[01;31m[K53[m[K5.txt

UltimatePOS 2.5 - Remote Code Execution
| php/webapps/452[01;31m[K53[m[K.txt

Umbraco CMS 7.12.4 - (Authenticated) Remote Code Execution
| aspx/webapps/461[01;31m[K53[m[K.py

UMI CMS 2.8.1.2 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K53[m[K28.txt

Unraid 6.8.0 - Auth Bypass PHP Code Execution (Metasploit)
| linux/remote/483[01;31m[K53[m[K.rb

UnrealIRCd 3.2.8.1 - Remote Downloader/Execute
| linux/remote/138[01;31m[K53[m[K.pl

Userlocator 3.0 - Blind SQL Injection
| php/webapps/7[01;31m[K53[m[K0.pl

Valarsoft WebMatic 3.0.5 - Multiple HTML Injection Vulnerabilities
| php/webapps/34[01;31m[K53[m[K5.txt

Valdersoft Shopping Cart 3.0 - Multiple Input Validation
Vulnerabilities                                    |
php/webapps/2[01;31m[K53[m[K01.txt
```

```
Vanilla Forums 2.0.17.x - 'p' Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K75.txt

Vastal I-Tech Software Zone - 'cat_id' SQL Injection
| php/webapps/[01;31m[K53[m[K59.txt

Venom Board - 'Post.php3' Multiple SQL Injections
| php/webapps/270[01;31m[K53[m[K.txt

VeryTools VideoSpirit Pro 1.70 - '.visprj' Local Buffer Overflow
(Metasploit)                                |
windows/local/171[01;31m[K53[m[K.rb

Vesta Control Panel 0.9.8-16 - Local Privilege Escalation
| linux/local/409[01;31m[K53[m[K.sh

ViArt Shop 4.0.5 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K53[m[K20.txt

VideoLAN VLC Media Player 2.2.1 - '.mp4' Heap Memory Corruption
| windows/dos/393[01;31m[K53[m[K.txt

Videos Broadcast Yourself 2 - 'UploadID' SQL Injection
| php/webapps/94[01;31m[K53[m[K.txt

VirtualBox 5.2.6.r120293 - VM Escape
| linux/local/4[01;31m[K53[m[K72.txt

VirtueMart - 'Product_ID' SQL Injection
| php/webapps/10[01;31m[K53[m[K3.txt

VisNetic ActiveDefense 1.3.1 - GET Multiple Denial of Service
Vulnerabilities                              |
multiple/dos/22[01;31m[K53[m[K5.txt

Visual Basic - 'vbe6.dll' Local Stack Overflow (PoC) / Denial of
Service                                     |
windows/dos/[01;31m[K53[m[K21.txt

Visual Ping 0.8.0.0 - 'Host' Denial of Service (PoC)
| windows_x86-64/dos/4[01;31m[K53[m[K16.py

visualpic 0.3.1 - Remote File Inclusion
| php/webapps/[01;31m[K53[m[K75.txt

VisualShapers EZContents 1.4/2.0 - 'module.php' Remote Command
Execution                                    |
php/webapps/23[01;31m[K53[m[K7.txt

Vitrax Pre-modded 1.0.6-r3 - Remote File Inclusion
| php/webapps/23[01;31m[K53[m[K.txt
```

```
VKPlayer 1.0 - '.mid' Denial of Service
| windows/dos/11[01;31m[K53[m[K4.pl

VMware vCenter Server 6.7 - Authentication Bypass
| multiple/webapps/48[01;31m[K53[m[K5.txt

VMware Workstation 12.5.2 - Drag n Drop Use-After-Free (Pwn2Own 2017)
(PoC)                                | windows/dos/44[01;31m[K53[m[K3.c

Vox TG790 ADSL Router - Cross-Site Scripting
| hardware/webapps/4[01;31m[K53[m[K10.txt

VP-ASP Shopping Cart - 'Shopadmin.asp' HTML Injection
| asp/webapps/26[01;31m[K53[m[K7.html

Vpop3d - Remote Denial of Service
| windows/dos/230[01;31m[K53[m[K.pl

VSAXESS V2.6.2.70 build 20171226_0[01;31m[K53[m[K - 'Nickname' Denial
of Service (PoC)                                    |
windows/dos/4[01;31m[K53[m[K15.py

VSAXESS V2.6.2.70 build20171226_0[01;31m[K53[m[K - 'organization'
Denial of Service (PoC)                                |
windows/dos/45800.py

VWar 1.5 - 'challenge.php?vwar_root' Remote File Inclusion
| php/webapps/283[01;31m[K53[m[K.txt

VX Search Enterprise 9.9.12 - 'Import Command' Local Buffer Overflow
| windows/local/42[01;31m[K53[m[K9.py

VyPRESS Messenger 3.5 - Remote Buffer Overflow
| windows/remote/246[01;31m[K53[m[K.txt

Vz (Adp) Forum 2.0.3 - Remote Password Disclosure
| php/webapps/30[01;31m[K53[m[K.txt

W-Agora 4.0 - 'delete_user.php?bn_dir_default' Remote File Inclusion
| php/webapps/314[01;31m[K53[m[K.txt

Warcraft III Replay Parser for PHP 1.8.c - 'index.php' Remote File
Inclusion                              |
php/webapps/27[01;31m[K53[m[K7.txt

Wavlink WN[01;31m[K53[m[K0HG4 - Password Disclosure
| hardware/webapps/50991.txt

Wavlink WN[01;31m[K53[m[K3A8 - Cross-Site Scripting (XSS)
| hardware/webapps/50989.txt

Wavlink WN[01;31m[K53[m[K3A8 - Password Disclosure
| hardware/webapps/50990.txt
```

WD My Cloud Mirror 2.11.1[01;31m[K53[m[K - Authentication Bypass / Remote Code Execution |
hardware/webapps/41147.txt

Web Cookbook - Multiple Vulnerabilities
| php/webapps/24[01;31m[K53[m[K1.txt

Web Wiz Forums 9.5 - Multiple SQL Injections
| asp/webapps/3[01;31m[K53[m[K10.txt

web@all 1.1 - 'url' Cross-Site Scripting
| php/webapps/352[01;31m[K53[m[K.txt

WebAsyst Shop-Script - Cross-Site Scripting / HTML Injection
| php/webapps/3[01;31m[K53[m[K19.txt

WebCT Discussion Board 4.1 - HTML Injection
| php/webapps/2[01;31m[K53[m[K81.txt

webERP 4.0.1 - 'InputSerialItemsFile.php' Arbitrary File Upload
| php/webapps/3[01;31m[K53[m[K33.py

WebfolioCMS 1.1.4 - Cross-Site Request Forgery (Add Admin/Modify Pages)
| php/webapps/18[01;31m[K53[m[K6.txt

WebKit - Universal XSS Using Cached Pages
| multiple/dos/474[01;31m[K53[m[K.txt

WebKit [01;31m[K53[m[K2.5 - Stack Exhaustion
| multiple/dos/12401.html

WebMaster ConferenceRoom 1.8 Developer Edition - Denial of Service
| multiple/dos/20[01;31m[K53[m[K4.txt

Webmedia Explorer 6.13.1 - Persistent Cross-Site Scripting
| php/webapps/1[01;31m[K53[m[K87.txt

Website Broker Script 3.02 - 'view' SQL Injection
| php/webapps/41[01;31m[K53[m[K9.txt

WebsiteBaker v2.13.3 - Stored XSS
| php/webapps/515[01;31m[K53[m[K.txt

webSPELL 4 - Authentication Bypass
| php/webapps/76[01;31m[K53[m[K.txt

webSPELL 4.2.0c - Bypass BBCode Cross-Site Scripting Cookie Stealing
| php/webapps/84[01;31m[K53[m[K.txt

Webspell 4.x - safe_query Bypass
| php/webapps/151[01;31m[K53[m[K.txt

WebWasher CSM 4.4.1 Build 752 Conf Script - Cross-Site Scripting
| cgi/webapps/2[01;31m[K53[m[K50.txt

WeChat for Android 7.0.4 - 'vcodec2_hls_filter' Denial of Service
| android/dos/468[01;31m[K53[m[K.txt

Wikipad 1.6.0 - Cross-Site Scripting / HTML Injection / Information
Disclosure |
php/webapps/3[01;31m[K53[m[K50.txt

Wikipedia 12.0 - Denial of Service (PoC)
| windows/dos/4[01;31m[K53[m[K24.py

Winamp - Playlist UNC Path Computer Name Overflow (Metasploit)
| windows/local/16[01;31m[K53[m[K1.rb

Winamp 5.5.8.2985 (in_mod plugin) - Local Stack Overflow
| windows/local/1[01;31m[K53[m[K12.py

Winamp 5.57 - 'Browser' IE Denial of Service
| windows/dos/11[01;31m[K53[m[K2.html

WinEggDropShell 1.7 - Multiple Remote Stack Overflows (PoC)
| windows/dos/13[01;31m[K53[m[K.py

WinMPG Video Convert 9.3.5 - Denial of Service
| windows/dos/465[01;31m[K53[m[K.py

Winn Guestbook 2.4 / Winn.ws - Cross-Site Scripting
| php/webapps/106[01;31m[K53[m[K.txt

WirelessHART Fieldgate SWG70 3.0 - Directory Traversal
| hardware/webapps/4[01;31m[K53[m[K42.txt

Wireshark 0.99.8 - LDAP Dissector Denial of Service
| linux/dos/315[01;31m[K53[m[K.txt

Wireshark 1.2.5 - LWRES getaddrbyname Buffer Overflow
| windows/remote/114[01;31m[K53[m[K.py

Wireshark 1.4.3 - '.pcap' Memory Corruption
| linux/remote/3[01;31m[K53[m[K14.txt

wodWebServer.NET 1.3.3 - Directory Traversal
| windows/remote/170[01;31m[K53[m[K.txt

Woltlab Burning Board Addon JGS-Treffen 2.0.2 - SQL Injection
| php/webapps/[01;31m[K53[m[K29.txt

Wondershare PDFelement 5.2.9 - Unquoted Service Path Privilege
Escalation |
windows/local/40[01;31m[K53[m[K5.txt

```
WordPress Core 2.5.1 - 'press-this.php' Multiple Cross-Site Scripting
Vulnerabilities                      |
php/webapps/320[01;31m[K53[m[K.txt

WordPress Plugin ADIF Log Search Widget - 'logbook_search.php' Cross-
Site Scripting                       |
php/webapps/38[01;31m[K53[m[K7.txt

WordPress Plugin BBPress 2.5 - Unauthenticated Privilege Escalation
| php/webapps/48[01;31m[K53[m[K4.py

WordPress Plugin Beer Recipes 1.0 - Cross-Site Scripting
| php/webapps/174[01;31m[K53[m[K.txt

WordPress Plugin CM Download Manager 2.0.0 - Code Injection
| php/webapps/3[01;31m[K53[m[K24.txt

WordPress Plugin ComicPress Manager 1.4.9 - 'lang' Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K93.txt

WordPress Plugin DB Backup - Arbitrary File Download
| php/webapps/3[01;31m[K53[m[K78.txt

WordPress Plugin Download - 'dl_id' SQL Injection
| php/webapps/[01;31m[K53[m[K26.txt

WordPress Plugin Download Manager 2.7.4 - Remote Code Execution
| php/webapps/35[01;31m[K53[m[K3.py

WordPress Plugin DukaPress 2.5.2 - Directory Traversal
| php/webapps/3[01;31m[K53[m[K46.txt

WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities
| php/webapps/395[01;31m[K53[m[K.txt

WordPress Plugin dzs-zoomsounds 6.60 - Remote Code Execution (RCE)
(Unauthenticated)                    |
php/webapps/507[01;31m[K53[m[K.py

WordPress Plugin Easy2Map 1.24 - SQL Injection
| php/webapps/37[01;31m[K53[m[K4.txt

WordPress Plugin ENL NewsLetter - '/wp-admin/admin.php' SQL Injection
| php/webapps/392[01;31m[K53[m[K.txt

WordPress Plugin Event Easy Calendar - Multiple Cross-Site Request
Forgery Vulnerabilities              |
php/webapps/387[01;31m[K53[m[K.html

WordPress Plugin Facebook Survey 1.0 - SQL Injection
| php/webapps/228[01;31m[K53[m[K.txt
```

WordPress Plugin Form Maker 1.12.24 - SQL Injection
| php/webapps/448[01;31m[K53[m[K.txt

WordPress Plugin GD Star Rating 1.9.7 - 'wpfn' Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K73.txt

WordPress Plugin Google Document Embedder 2.5.14 - SQL Injection
| php/webapps/3[01;31m[K53[m[K71.txt

WordPress Plugin GraceMedia Media Player 1.0 - Local File Inclusion
| php/webapps/46[01;31m[K53[m[K7.txt

WordPress Plugin Hms Testimonials 2.0.10 - Multiple Vulnerabilities
| php/webapps/27[01;31m[K53[m[K1.txt

WordPress Plugin IGIT Posts Slider Widget 1.0 - 'src' Cross-Site
Scripting |
php/webapps/3[01;31m[K53[m[K92.txt

WordPress Plugin Jibu Pro 1.7 - Cross-Site Scripting
| php/webapps/4[01;31m[K53[m[K05.txt

WordPress Plugin Like Dislike Counter 1.2.3 - SQL Injection
| php/webapps/345[01;31m[K53[m[K.txt

WordPress Plugin Multi-Scheduler 1.0.0 - Cross-Site Request Forgery
(Delete User) |
php/webapps/48[01;31m[K53[m[K2.txt

WordPress Plugin Nmedia WordPress Member Conversation 1.35.0 -
'doupload.php' Arbitrary File Upload |
php/webapps/373[01;31m[K53[m[K.php

WordPress Plugin Paid Memberships Pro 1.7.14.2 - Directory Traversal
| php/webapps/3[01;31m[K53[m[K03.txt

WordPress Plugin Paypal Currency Converter Basic For WooCommerce - File
Read | php/webapps/372[01;31m[K53[m[K.txt

WordPress Plugin Premium Gallery Manager - Configuration Access
| php/webapps/34[01;31m[K53[m[K8.txt

WordPress Plugin Pyrmont 2.x - SQL Injection
| php/webapps/10[01;31m[K53[m[K5.txt

WordPress Plugin Quizlord 2.0 - Cross-Site Scripting
| php/webapps/4[01;31m[K53[m[K07.txt

WordPress Plugin Rich Widget - Arbitrary File Upload
| php/webapps/376[01;31m[K53[m[K.txt

WordPress Plugin Simple Image Manipulator 1.0 - Arbitrary File Download
| php/webapps/377[01;31m[K53[m[K.txt

```
WordPress Plugin Slider REvolution 3.0.95 / Showbiz Pro 1.7.1 -
Arbitrary File Upload                        |
php/webapps/3[01;31m[K53[m[K85.pl

Wordpress Plugin Smart Product Review 1.0.4 - Arbitrary File Upload
| php/webapps/50[01;31m[K53[m[K3.py

WordPress Plugin SP Client Document Manager 2.4.1 - SQL Injection
| php/webapps/3[01;31m[K53[m[K13.txt

WordPress Plugin st_newsletter - SQL Injection
| php/webapps/50[01;31m[K53[m[K.txt

WordPress Plugin Supsystic Newsletter 1.5.5 - 'sidx' SQL injection
| php/webapps/49[01;31m[K53[m[K9.txt

WordPress Plugin Supsystic Pricing Table 1.8.7 - Multiple
Vulnerabilities                                |
php/webapps/49[01;31m[K53[m[K3.txt

WordPress Plugin Supsystic Ultimate Maps 1.1.12 - 'sidx' SQL injection
| php/webapps/49[01;31m[K53[m[K2.txt

WordPress Plugin TagNinja 1.0 - 'id' Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K00.txt

WordPress Plugin Top Quark Architecture 2.10 - Arbitrary File Upload
| php/webapps/190[01;31m[K53[m[K.txt

WordPress Plugin Welcart e-Commerce 2.0.0 - 'search[order_column][0]'
SQL injection                          |
php/webapps/49[01;31m[K53[m[K1.txt

WordPress Plugin WP E-Commerce Shop Styling 2.5 - Arbitrary File
Download                                   |
php/webapps/37[01;31m[K53[m[K0.txt

WordPress Plugin wp-autoyoutube - Blind SQL Injection
| php/webapps/183[01;31m[K53[m[K.txt

WordPress Plugin wpDataTables 1.5.3 - Arbitrary File Upload
| php/webapps/3[01;31m[K53[m[K41.py

WordPress Plugin wpDataTables 1.5.3 - SQL Injection
| php/webapps/3[01;31m[K53[m[K40.txt

WordPress Plugin YT-Audio 1.7 - 'v' Cross-Site Scripting
| php/webapps/3[01;31m[K53[m[K94.txt

WordPress Theme Area[01;31m[K53[m[K - Arbitrary File Upload
| php/webapps/29068.txt
```

```
WordPress Theme classipress 3.1.4 - Persistent Cross-Site Scripting
| php/webapps/180[01;31m[K53[m[K.txt

WordPress Theme Medic v1.0.0 - Weak Password Recovery Mechanism for
Forgotten Password                      |
php/webapps/51[01;31m[K53[m[K1.py

WordPress Theme SiteMile Project 2.0.9.5 - Multiple Vulnerabilities
| php/webapps/39[01;31m[K53[m[K6.txt

Working Resources BadBlue Server 2.40 - 'PHPtest.php' Full Path
Disclosure                                 |
php/webapps/237[01;31m[K53[m[K.txt

WorkingOnWeb 2.0.1400 - 'events.php' SQL Injection
| php/webapps/46[01;31m[K53[m[K.txt

WP Sticky Social 1.0.1 - Cross-Site Request Forgery to Stored Cross-
Site Scripting (XSS)                    |
php/webapps/51[01;31m[K53[m[K3.py

WSN Guest 1.24 - 'wsnuser' Cookie SQL Injection
| php/webapps/3[01;31m[K53[m[K60.txt

WSO2 Carbon / WSO2 Dashboard Server 5.3.0 - Persistent Cross-Site
Scripting                                  |
java/webapps/44[01;31m[K53[m[K1.txt

X-Changer 0.20 - Multiple SQL Injections
| php/webapps/27[01;31m[K53[m[K3.txt

XAMPP - 'Phonebook.php' Multiple Remote HTML Injection Vulnerabilities
| multiple/remote/2[01;31m[K53[m[K91.txt

XAMPP - Insecure Default Password Disclosure
| multiple/dos/2[01;31m[K53[m[K93.txt

XAMPP 1.7.3 - Multiple Vulnerabilities
| php/webapps/1[01;31m[K53[m[K70.txt

XBMC 9.04.1r20672 - 'soap_action_name' POST UPnP 'sscanf' Remote Buffer
Overflow                              |
windows/remote/1[01;31m[K53[m[K47.py

xEpan 1.0.1 - Cross-Site Request Forgery
| php/webapps/3[01;31m[K53[m[K81.txt

xEpan 1.0.4 - Multiple Vulnerabilities
| php/webapps/3[01;31m[K53[m[K96.txt

Xerox 4595 - Denial of Service
| hardware/dos/1[01;31m[K53[m[K80.py
```

Xfinity Gateway - Cross-Site Request Forgery
| hardware/webapps/408[01;31m[K53[m[K.txt

Xion Audio Player 1.0.126 - Unicode Stack Buffer Overflow (Metasploit)
| windows/local/166[01;31m[K53[m[K.rb

Xitami Web Server 2.5c2 - If-Modified-Since Overflow (Metasploit)
| windows/remote/167[01;31m[K53[m[K.rb

Xitami Web Server 2.5c2 - LRWP Processing Format String (PoC)
| windows/dos/[01;31m[K53[m[K54.c

Xnami 1.0 - Cross-Site Scripting
| php/webapps/43[01;31m[K53[m[K5.txt

XnView 1.92.1 - 'FontName' Slideshow Buffer Overflow
| windows/local/[01;31m[K53[m[K46.pl

Xoops 1.3.x/2.0 MyTextSanitizer - HTML Injection
| php/webapps/22[01;31m[K53[m[K9.txt

XOOPS 2.5.4 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/187[01;31m[K53[m[K.txt

XPOZE Pro 3.05 - 'reed' SQL Injection
| php/webapps/[01;31m[K53[m[K58.pl

YaBBSM 3.0.0 - 'Offline.php' Remote File Inclusion
| php/webapps/25[01;31m[K53[m[K.txt

Yager 5.24 - Remote Buffer Overflow
| windows/remote/9[01;31m[K53[m[K.c

Yahoo! Messenger 8.0 - Notification Message HTML Injection
| windows/dos/29[01;31m[K53[m[K1.txt

Yahoo! Messenger Webcam 8.1 - 'Ywcupl.dll' Download / Execute
| windows/remote/40[01;31m[K53[m[K.c

Yappa-ng 1.x/2.x - Cross-Site Scripting
| php/webapps/25[01;31m[K53[m[K3.txt

Yappa-ng 1.x/2.x - Remote File Inclusion
| php/webapps/25[01;31m[K53[m[K2.txt

Yaws 1.89 - Directory Traversal
| windows/remote/1[01;31m[K53[m[K71.txt

YeaLink SIP-TXXXP [01;31m[K53[m[K.84.0.15 - 'cmd' Command Injection
(Authenticated) |
hardware/webapps/50509.txt

```
YepYep MTFTPD 0.2/0.3 - Remote CWD Argument Format String
| linux/remote/2[01;31m[K53[m[K21.c

YetiShare File Hosting Script 5.1.0 - 'url' Server-Side Request Forgery
| php/webapps/49[01;31m[K53[m[K4.txt

YouTube Automated CMS 1.0.7 - Cross-Site Request Forgery / Persistent
Cross-Site Scripting                 |
php/webapps/40[01;31m[K53[m[K4.html

yPlay 2.4.5 - Denial of Service
| windows/dos/1[01;31m[K53[m[K56.pl

Yvora CMS 1.0 - 'error_view.php?ID' SQL Injection
| php/webapps/43[01;31m[K53[m[K.txt

Zabbix 2.0 < 3.0.3 - SQL Injection
| php/webapps/403[01;31m[K53[m[K.py

Zenario CMS 8.8.[01;31m[K53[m[K370 - 'id' Blind SQL Injection
| php/webapps/49642.txt

Zenmap (Nmap) 7.70 - Denial of Service (PoC)
| windows_x86/dos/4[01;31m[K53[m[K57.txt

Zenoss 2.3.3 - Multiple Cross-Site Request Forgery Vulnerabilities
| multiple/remote/33[01;31m[K53[m[K6.txt

Zenturi NixonMyPrograms Class 'sasatl.dll 1.5.0.[01;31m[K53[m[K1' -
Remote Buffer Overflow                                  |
windows/remote/4214.html

Zeus Web Server 4.x - 'SSL2_CLIENT_HELLO' Remote Buffer Overflow (PoC)
| multiple/dos/33[01;31m[K53[m[K1.py

ZHONE < S3.0.501 - Multiple Vulnerabilities
| hardware/remote/384[01;31m[K53[m[K.txt

Zimbra 8.6.0_GA_11[01;31m[K53[m[K - Cross-Site Scripting
| php/webapps/45177.txt

ZipCentral - '.zip' File (SEH)
| windows/local/120[01;31m[K53[m[K.py

Zomplog 3.9 - Cross-Site Request Forgery
| php/webapps/1[01;31m[K53[m[K29.txt

Zomplog 3.9 - Multiple Cross-Site Scripting / Cross-Site Request
Forgery Vulnerabilities                    |
php/webapps/1[01;31m[K53[m[K31.txt

Zoom Media Gallery 2.1.2 - 'index.php' SQL Injection
| php/webapps/2[01;31m[K53[m[K79.txt
```

Zoom Telephonics ADSL Modem/Router - Multiple Vulnerabilities
| hardware/webapps/280[01;31m[K53[m[K.txt

Zoopeer 0.1/0.2 - 'FCKeditor' Arbitrary File Upload
| php/webapps/1[01;31m[K53[m[K54.txt

ZTE Modem ZXDSL [01;31m[K53[m[K1BIIV7.3.0f_D09_IN - Persistent Cross-Site Scripting |
hardware/webapps/35128.txt

Zurmo CRM - Persistent Cross-Site Scripting
| php/webapps/339[01;31m[K53[m[K.txt

Zyke CMS 1.1 - Bypass
| php/webapps/124[01;31m[K53[m[K.txt

ZYXEL PMG[01;31m[K53[m[K18-B20A - OS Command Injection
| hardware/webapps/38455.txt

µTorrent (uTorrent) 1.8.3 Build 15772 - Create New Torrent Buffer Overflow (PoC) |
windows/dos/9[01;31m[K53[m[K9.py

Shellcode Title
| Path

Android/ARM - Reverse (10.0.2.2:0x3412/TCP) Shell (/system/bin/sh) Shellcode (79 bytes) | arm/43[01;31m[K53[m[K6.c

BSD/x86 - setuid(0) + Break chroot (../ 10x Loop) Shellcode (46 bytes)
| bsd_x86/134[01;31m[K53[m[K.c

Linux/ARM (Raspberry Pi) - execve(_/bin/sh__ [0]_ [0 vars]) Shellcode (30 bytes) | arm/212[01;31m[K53[m[K.asm

Linux/ARM - execve(_/bin/sh__ NULL_ NULL) + read(0_ buf_ 0xff) Stager Shellcode (28 Bytes) | arm/4[01;31m[K53[m[K08.c

Linux/ARM - Add Map (127.1.1.1 google.lk) To /etc/hosts Shellcode (79 bytes) | arm/43[01;31m[K53[m[K0.c

Linux/ARM - Bind (0x1337/TCP) Listener + Receive + Payload Loader Shellcode | arm/1[01;31m[K53[m[K16.asm

Linux/ARM - Bind (0x1337/TCP) Shell Shellcode
| arm/1[01;31m[K53[m[K14.asm

Linux/ARM - Bind (68/UDP) Listener + Reverse (192.168.0.1:67/TCP) Shell
Shellcode | arm/1[01;31m[K53[m[K15.asm

Linux/ARM - chmod(/etc/passwd 0777) Shellcode (39 bytes)
| arm/43[01;31m[K53[m[K1.c

Linux/ARM - creat(_/root/pwned__ 0777) Shellcode (39 bytes)
| arm/43[01;31m[K53[m[K2.c

Linux/ARM - execve(_/bin/sh__ NULL_ NULL) + read(0_ buf_ 0xff) Stager
Shellcode (20 Bytes) | arm/4[01;31m[K53[m[K29.c

Linux/ARM - execve(_/bin/sh__ []_ [0 vars]) Shellcode (35 bytes)
| arm/43[01;31m[K53[m[K3.c

Linux/ARM - execve(_/bin/sh__NULL_0) Shellcode (31 bytes)
| arm/43[01;31m[K53[m[K4.c

Linux/ARM - ifconfig eth0 192.168.0.2 up Shellcode
| arm/1[01;31m[K53[m[K17.asm

Linux/ARM64 - Read /etc/passwd Shellcode (120 Bytes)
| arm/470[01;31m[K53[m[K.c

Linux/StrongARM - Bind (/TCP) Shell (/bin/sh) Shellcode (203 bytes)
| arm/43[01;31m[K53[m[K9.c

Linux/StrongARM - execve(/bin/sh) Shellcode (47 bytes)
| arm/43[01;31m[K53[m[K8.c

Linux/StrongARM - setuid() Shellcode (20 bytes)
| arm/43[01;31m[K53[m[K7.c

Linux/x64 - Egghunter (0xbeefbeef) Shellcode (34 bytes)
| linux_x86-64/439[01;31m[K53[m[K.nasm

Linux/x64 - Flush IPTables Rules (execve(_/sbin/iptables__
[_/sbin/iptables__ _-F_]_ NULL)) Shellcode (43 | linux_x86-
64/435[01;31m[K53[m[K.c

Linux/x64 - Reverse (192.168.1.2:4444/TCP) Shell Shellcode
(1[01;31m[K53[m[K bytes) |
linux_x86-64/42485.c

Linux/x86 - /etc/init.d/apparmor teardown Shellcode ([01;31m[K53[m[K
bytes) | linux_x86/43705.c

Linux/x86 - Bind (43690/TCP) + Null-Free Shellcode ([01;31m[K53[m[K
Bytes) | linux_x86/47396.c

Linux/x86 - Bind (64[01;31m[K53[m[K3/TCP) Shell (/bin/sh) Shellcode (97 bytes) | linux_x86/14216.c

Linux/x86 - chmod 0777 /etc/shadow + Obfuscated Shellcode (51 bytes) | linux_x86/437[01;31m[K53[m[K.c

Linux/x86 - chmod(/etc/shadow_ 0666) + Polymorphic Shellcode ([01;31m[K53[m[K bytes) | linux_x86/47200.c

Linux/x86 - execve() - Terminal Calculator (bc) Shellcode ([01;31m[K53[m[K bytes) | linux_x86/46275.c

Linux/x86 - execve() Shellcode (51 bytes) | linux_x86/135[01;31m[K53[m[K.c

Linux/x86 - execve(/bin/sh) + MMX/ROT13/XOR Shellcode (Encoder/Decoder) (104 bytes) | linux_x86/45[01;31m[K53[m[K8.txt

Linux/x86 - execve(/bin/sh) + Polymorphic Shellcode ([01;31m[K53[m[K bytes) | linux_x86/43489.c

Linux/x86 - execve(/bin/sh) Socket Reuse Shellcode (42 bytes) | linux_x86/47[01;31m[K53[m[K0.txt

Linux/x86 - execve(/sbin/shutdown_/sbin/shutdown 0) Shellcode (36 bytes) | linux_x86/436[01;31m[K53[m[K.c

Linux/x86 - Reverse (127.0.0.1:[01;31m[K53[m[K/UDP) Shell (/bin/sh) Shellcode (668 bytes) | linux_x86/42208.nasm

Linux/x86 - Reverse (140.115.[01;31m[K53[m[K.35:9999/TCP) + Download File (cb) + Execute Shellcode (149 bytes) | linux_x86/13337.c

Linux/x86 - setreuid(0_0) + execve(_/bin/csh__ [/bin/csh_ NULL]) + XOR Encoded Shellcode ([01;31m[K53[m[K bytes) | linux_x86/43711.py

Linux/x86 - setreuid(0_0) + execve(_/bin/ksh__ [/bin/ksh_ NULL]) + XOR Encoded Shellcode ([01;31m[K53[m[K bytes) | linux_x86/43712.py

Linux/x86 - setreuid(0_0) + execve(_/bin/zsh__ [/bin/zsh_ NULL]) + XOR Encoded Shellcode ([01;31m[K53[m[K bytes) | linux_x86/43714.py

Linux/x86 - setuid(0) + execve(/bin/sh) Shellcode (28 bytes) | linux_x86/133[01;31m[K53[m[K.c

Windows (XP SP1) - Bind (58821/TCP) Shell Shellcode (116 bytes) | windows_x86/13[01;31m[K53[m[K1.c

Windows (XP) - Download File (http://www.elitehaven.net/ncat.exe) + Execute (nc.exe) + Null-Free Shellcode | windows_x86/13[01;31m[K53[m[K0.asm

Windows (XP/2000/2003) - Reverse (127.0.0.1:[01;31m[K53[m[K/TCP) Shell Shellcode (275 bytes) (Generator) | generator/13528.c

Windows (XP/Vista/7) - Egghunter (0x07333[01;31m[K53[m[K1) JITed Stage-0 Adjusted Universal Shellcode | windows/13649.as

Windows - DCOM RPC2 Universal Shellcode | windows_x86/13[01;31m[K53[m[K2.asm

Windows - Egghunter (0x07333[01;31m[K53[m[K1) JITed Stage-0 Shellcode | windows/13645.c

Windows/x64 (7) - Screen Lock Shellcode (9 bytes) | windows_x86-64/479[01;31m[K53[m[K.c

Windows/x64 - URLDownloadToFileA(http://localhost/trojan.exe) + Execute Shellcode (218+ bytes) | windows_x86-64/13[01;31m[K53[m[K3.asm

Windows/x86 (XP SP3) (Turkish) - calc.exe Shellcode ([01;31m[K53[m[K bytes) | windows_x86/43770.c

Windows/x86 - CreateProcessA cmd.exe Shellcode (2[01;31m[K53[m[K bytes) | windows_x86/40246.c

---

Port: 5357

Exploit Title | Path

Advantech EKI-6340 - Command Injection | cgi/webapps/3[01;31m[K5357[m[K.txt

CubeCart 2.0.x - 'view_cart.php?add' Full Path Disclosure | php/webapps/2[01;31m[K5357[m[K.txt

Home FTP Server 1.11.1.149 - 'RETR'/'DELE'/'RMD' Directory Traversal | windows/remote/1[01;31m[K5357[m[K.php

SCO UnixWare Merge - 'mcd' Local Privilege Escalation
| sco/local/[01;31m[K5357[m[K.c

Zenmap (Nmap) 7.70 - Denial of Service (PoC)
| windows_x86/dos/4[01;31m[K5357[m[K.txt

Shellcodes: No Results

Port: 54253

Exploits: No Results

Shellcodes: No Results

Port: 5432

Exploit Title
| Path

LeadTools 11.5.0.9 - 'ltisi11n.ocx' DriverName() Access Violation
Denial of Service |
windows/dos/1[01;31m[K5432[m[K.html

Microsoft Edge Chakra JIT - 'localeCompare' Type Confusion
| windows/dos/4[01;31m[K5432[m[K.js

PHPAddressBook 2.11 - 'view.php' SQL Injection
| php/webapps/[01;31m[K5432[m[K.txt

phpBB Remote - 'mod.php' SQL Injection
| php/webapps/2[01;31m[K5432[m[K.txt

Wireshark 1.4.3 - NTLMSSP Null Pointer Dereference Denial of Service
| linux/dos/3[01;31m[K5432[m[K.txt

Shellcode Title
| Path

Linux/x86 - Reverse (192.168.3.119:[01;31m[K5432[m[K1/TCP) Shell
(/bin/bash) Shellcode (110 bytes) |
linux_x86/41723.c

Linux/x86 - Reverse ([01;31m[K5432[m[K1/UDP) tcpdump Live Packet
Capture Shellcode (151 bytes) |
linux_x86/13329.c

Port: 5900

Exploit Title
| Path

Barracuda Networks Cloud Series - Filter Bypass
| cgi/webapps/3[01;31m[K5900[m[K.txt

RSS-aggregator - 'path' Remote File Inclusion
| php/webapps/[01;31m[K5900[m[K.txt

UBBCentral UBB.Threads 5.5.1/6.x - 'viewmessage.php?message' SQL
Injection |
php/webapps/2[01;31m[K5900[m[K.txt

WordPress Plugin Easy Testimonials 3.2 - Cross-Site Scripting
| php/webapps/4[01;31m[K5900[m[K.txt

Shellcodes: No Results

Port: 59447

Exploits: No Results

Shellcodes: No Results

Port: 59865

Exploits: No Results

Shellcodes: No Results

Port: 6000

Exploit Title
| Path

Asus AAM6330BI/AAM[01;31m[K6000[m[KEV ADSL Router - Information Disclosure |
hardware/remote/22898.txt

CIK Telecom VoIP Router SVG[01;31m[K6000[m[KRW - Privilege Escalation / Command Execution |
hardware/webapps/35556.txt

Cisco Catalyst 4000 4.x/5.x / Catalyst 5000 4.5/5.x / Catalyst [01;31m[K6000[m[K 5.x - Memory Leak Denial of Service |
hardware/dos/20473.pl

Cisco Catalyst 4000/5000/[01;31m[K6000[m[K 6.1 - SSH Protocol Mismatch Denial of Service |
hardware/dos/20509.pl

GL-iNet MT[01;31m[K6000[m[K 4.5.5 - Arbitrary File Download
| hardware/remote/51942.py

HP Network Automation 9.10 - SQL Injection
| php/webapps/3[01;31m[K6000[m[K.txt

NVIDIA Driver - Unchecked Write to User-Provided Pointer in Escape 0x[01;31m[K6000[m[K00D |
windows/dos/40659.txt

pHNews CMS Alpha 1 - Local File Inclusion
| php/webapps/[01;31m[K6000[m[K.txt

Samsung D[01;31m[K6000[m[K TV - Multiple Vulnerabilities
| hardware/dos/18751.txt

SDL Web Content Manager 8.5.0 - XML External Entity Injection
| xml/webapps/4[01;31m[K6000[m[K.txt

Seo Panel 2.2.0 - Cookie-Rendered Persistent Cross-Site Scripting
| php/webapps/1[01;31m[K6000[m[K.txt

Shellcodes: No Results

Port: 7070

Exploit Title
| Path

Interspire TrackPoint NX - 'index.php' Cross-Site Scripting
| php/webapps/2[01;31m[K7070[m[K.txt

Mac OS X TimeMachine - 'tmdiagnose' Command Injection Privilege Escalation (Metasploit) |
macos/local/4[01;31m[K7070[m[K.rb

PRO-[01;31m[K7070[m[K Hazır Profesyonel Web Sitesi 1.0 - Authentication Bypass | php/webapps/47758.txt

Rumble 0.25.2232 - Denial of Service
| windows/dos/1[01;31m[K7070[m[K.py

WordPress Plugin Uploadify Integration 0.9.6 - Multiple Cross-Site Scripting Vulnerabilities |
php/webapps/3[01;31m[K7070[m[K.txt

Zeeways PHOTOVIDEOTUBE 1.1 - Authentication Bypass
| php/webapps/[01;31m[K7070[m[K.txt

Shellcodes: No Results

Port: 80

Exploit Title
| Path

.NET Remoting Services - Remote Command Execution
| windows/remote/352[01;31m[K80[m[K.txt

1024 CMS 1.1.0 Beta - 'force_download.php' Local File Inclusion
| php/webapps/1[01;31m[K80[m[K00.txt

1024 CMS 1.4.4 - Remote Command Execution / Remote File Inclusion
| php/webapps/[01;31m[K80[m[K03.pl

11in1 CMS 1.0.1 - 'do.php' CRLF Injection
| php/webapps/1[01;31m[K80[m[K95.txt

321soft PHP-Gallery 0.9 - 'index.php?path' Arbitrary Directory Listing
| php/webapps/27[01;31m[K80[m[K3.txt

321soft PHP-Gallery 0.9 - 'index.php?path' Cross-Site Scripting
| php/webapps/27[01;31m[K80[m[K4.txt

3Com OfficeConnect Routers - 'Content-Type' Denial of Service
| hardware/dos/105[01;31m[K80[m[K.rb

3Com OfficeConnect Wireless Cable/DSL Router - Authentication Bypass
| hardware/remote/[01;31m[K80[m[K22.txt

3Com* iMC (Intelligent Management Center) - Cross-Site Scripting /
Information Disclosure Flaws |
windows/webapps/126[01;31m[K80[m[K.txt

4Images 1.7.1 - 'top.php?sessionid' SQL Injection
| php/webapps/277[01;31m[K80[m[K.txt

A Better Member-Based ASP Photo Gallery - 'entry' SQL Injection
| php/webapps/[01;31m[K80[m[K12.txt

A4Desk Event Calendar - 'eventid' SQL Injection
| php/webapps/32[01;31m[K80[m[K3.txt

aaPanel 6.8.21 - Directory Traversal (Authenticated)
| linux/webapps/507[01;31m[K80[m[K.txt

```
Aastra IP Phone 94[01;31m[K80[m[Ki - Web Interface Data Disclosure
| hardware/webapps/17376.txt

ABB Cylon FLXeon 9.3.4 - Cross-Site Request Forgery
| multiple/hardware/521[01;31m[K80[m[K.txt

AbsoluteTelnet 11.12 - 'license name' Denial of Service (PoC)
| windows/dos/4[01;31m[K80[m[K06.py

AbsoluteTelnet 11.12 - 'SSH2/username' Denial of Service (PoC)
| windows/dos/4[01;31m[K80[m[K10.py

AbsoluteTelnet 11.12 - _license name_ Denial of Service (PoC)
| windows/dos/4[01;31m[K80[m[K05.py

Abuse 2.0 - Local Buffer Overflow
| linux/local/219[01;31m[K80[m[K.c

Accela Civic Platform 21.1 - 'servProvCode' Cross-Site-Scripting (XSS)
| multiple/webapps/499[01;31m[K80[m[K.txt

AceFTP 3.[01;31m[K80[m[K.3 - 'LIST' Directory Traversal
| windows/remote/31997.txt

ACGV News 0.9.1 - 'glossaire.php?id' Cross-Site Scripting
| php/webapps/31[01;31m[K80[m[K2.txt

ACGV News 0.9.1 - 'glossaire.php?id' SQL Injection
| php/webapps/31[01;31m[K80[m[K1.txt

Acritum Femitter Server 1.03 - Multiple Vulnerabilities
| windows/remote/124[01;31m[K80[m[K.txt

Acronis True Image Echo Enterprise Server 9.5.0.[01;31m[K80[m[K72 -
Multiple Remote Denial of Service Vulnerabilities   |
multiple/dos/31376.txt

Active Business Directory 2 - 'searchadvance.asp' Cross-Site Scripting
| asp/webapps/343[01;31m[K80[m[K.txt

Active NewsLetter 4.3 - Authentication Bypass
| asp/webapps/72[01;31m[K80[m[K.txt

ActivePerl 5.8.8.817 - Local Buffer Overflow
| windows/local/13[01;31m[K80[m[K6.txt

ActiveState Perl.exe x64 Client 5.20.2 - Crash (PoC)
| windows_x86-64/dos/3[01;31m[K80[m[K85.pl

AdaptCMS Lite 1.4 - Cross-Site Scripting / Remote File Inclusion
| php/webapps/[01;31m[K80[m[K16.txt
```

Adaptive Website Framework 1.11 - Remote File Inclusion
| php/webapps/2[01;31m[K80[m[K08.txt

Admin Express 1.2.5.485 - 'Folder Path' Local SEH Alphanumeric Encoded
Buffer Overflow |
windows/local/46[01;31m[K80[m[K5.py

Adobe Acrobat Reader - JBIG2 Local Buffer Overflow (PoC) (2)
| windows/dos/[01;31m[K80[m[K99.pl

Adobe Acrobat Reader - JBIG2 Universal
| windows/local/82[01;31m[K80[m[K.txt

Adobe Dreamweaver CS4 - 'mfc[01;31m[K80[m[Kesn.dll' DLL Loading
Arbitrary Code Execution |
windows/remote/34829.c

Adobe Flash - Heap Buffer Overflow Due to Indexing Error When Loading
FLV File | linux_x86-
64/dos/378[01;31m[K80[m[K.txt

Adobe Flash - Invoke Accesses Trait Out-of-Bounds
| windows/dos/424[01;31m[K80[m[K.txt

Adobe Flash Player - copyPixelsToByteArray Integer Overflow
(Metasploit) |
windows/remote/36[01;31m[K80[m[K8.rb

Adobe Flash Player - UncompressViaZlibVariant Uninitialized Memory
(Metasploit) |
windows/remote/368[01;31m[K80[m[K.rb

Adobe Flex SDK 3.x - 'index.template.html' Cross-Site Scripting
| multiple/webapps/331[01;31m[K80[m[K.txt

Adobe Photoshop Elements 8.0 - Active File Monitor Privilege Escalation
| windows/local/9[01;31m[K80[m[K7.txt

Advanced File Vault - 'eSellerateControl350.dll' ActiveX HeapSpray
| windows/remote/145[01;31m[K80[m[K.html

Advanced Poll 2.02 - SQL Injection
| php/webapps/1[01;31m[K80[m[K76.txt

Advantech WebAccess 8.2-2017.03.31 - Webvrpcs Service Opcode
[01;31m[K80[m[K061 Stack Buffer Overflow (Metasploit) |
windows/webapps/43340.rb

AgerMenu 0.01 - 'top.inc.php?rootdir' Remote File Inclusion
| php/webapps/32[01;31m[K80[m[K.txt

```
Ahsay Backup 7.x - 8.1.1.50 - Authenticated Arbitrary File Upload /
Remote Code Execution (Metasploit)     |
jsp/webapps/471[01;31m[K80[m[K.rb

aidiCMS 3.55 - 'ajax_create_folder.php' Remote Code Execution
| php/webapps/1[01;31m[K80[m[K85.php

AIMP2 Audio Converter 2.53 build 330 - Playlist '.pls' Unicode Buffer
Overflow                              |
windows/local/102[01;31m[K80[m[K.py

Aircrack-NG 0.7 - 'Specially Crafted [01;31m[K80[m[K2.11 Packets'
Remote Buffer Overflow                                  |
linux/remote/3724.c

Aj Classifieds Real Estate 3.0 - Arbitrary File Upload
| php/webapps/7[01;31m[K80[m[K9.txt

Ajax File and Image Manager 1.0 Final - Remote Code Execution
| php/webapps/1[01;31m[K80[m[K75.txt

AKCP sensorProbe SPX476 - 'Multiple' Cross-Site Scripting (XSS)
| hardware/webapps/500[01;31m[K80[m[K.txt

Aktiv Player 2.[01;31m[K80[m[K - Crash (PoC)
| windows/dos/237[01;31m[K80[m[K.py

Alex DownloadEngine 1.4.1 - 'comments.php' SQL Injection
| php/webapps/279[01;31m[K80[m[K.txt

Algo [01;31m[K80[m[K28 Control Panel - Remote Code Execution (RCE)
(Authenticated)                                         |
hardware/remote/50960.py

Alienvault Open Source SIEM (OSSIM) 3.1 - Multiple Vulnerabilities
| php/webapps/18[01;31m[K80[m[K0.txt

Alienvault Open Source SIEM (OSSIM) < 4.7.0 - av-centerd
'get_log_line()' Remote Code Execution            |
linux/remote/33[01;31m[K80[m[K5.pl

AlkalinePHP 0.[01;31m[K80[m[K.00 Beta - 'thread.php' SQL Injection
| php/webapps/5652.pl

AlsaPlayer < 0.99.[01;31m[K80[m[K-rc3 - Vorbis Input Local Buffer
Overflow                                                |
linux/local/5424.txt

Alt-N SecurityGateway 1.0.1 - 'Username' Remote Buffer Overflow
(Metasploit)                                  |
windows/remote/16[01;31m[K80[m[K3.rb
```

```
AM4SS 1.2 - Cross-Site Request Forgery (Add Admin)
| php/webapps/17[01;31m[K80[m[K0.txt

AN Guestbook 0.4 - 'send_email.php' Cross-Site Scripting
| php/webapps/31[01;31m[K80[m[K3.txt

Android Gmail < 7.11.5.17656[01;31m[K80[m[K39 - Directory Traversal in
Attachment Download                              | android/dos/43189.py

Andy Mack 35mm Slide Gallery 6.0 - 'index.php?imgdir' Cross-Site
Scripting                                        |
php/webapps/2[01;31m[K80[m[K20.txt

Andy Mack 35mm Slide Gallery 6.0 - 'popup.php' Multiple Cross-Site
Scripting Vulnerabilities                        |
php/webapps/2[01;31m[K80[m[K21.txt

Angora Guestbook 1.5 - Local File Inclusion
| php/webapps/173[01;31m[K80[m[K.txt

Anviz CrossChex - Buffer Overflow (Metasploit)
| windows/remote/4[01;31m[K80[m[K92.rb

Apache mod_rewrite (Windows x86) - Off-by-One Remote Overflow
| windows_x86/remote/36[01;31m[K80[m[K.sh

Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow
(2)                                  | unix/remote/470[01;31m[K80[m[K.c

Apache Struts - includeParams Remote Code Execution (Metasploit)
| multiple/remote/259[01;31m[K80[m[K.rb

ApowerManager 3.1.7 - Phone Manager Remote Denial of Service (PoC)
| android/dos/463[01;31m[K80[m[K.py

Apple Airport - [01;31m[K80[m[K2.11 Probe Response Kernel Memory
Corruption (PoC) (Metasploit)                    |
hardware/dos/2700.rb

Apple iOS 10.2 - Broadcom Out-of-Bounds Write when Handling
[01;31m[K80[m[K2.11k Neighbor Report Response                |
ios/remote/42784.txt

Apple iOS Safari - 'JS .' Remote Crash
| hardware/dos/15[01;31m[K80[m[K5.php

Apple Mac OSX - OSMetaClassBase::safeMetaCast in
IOAccelContext2::connectClient NULL Dereference           |
osx/dos/393[01;31m[K80[m[K.c

Apple Mac OSX Adobe Version Cue - Local Privilege Escalation
| osx/local/6[01;31m[K80[m[K.txt
```

Apple Mac OSX Entitlements - 'Rootpipe' Local Privilege Escalation (Metasploit) | osx/local/3[01;31m[K80[m[K36.rb

Apple macOS/iOS Kernel 10.12.3 (16D32) - Double-Free Due to Bad Locking in fsevents Device | multiple/local/41[01;31m[K80[m[K4.c

Apple QuickTime < 7.7.79.[01;31m[K80[m[K.95 - '.FPX' Parsing Memory Corruption (1) | multiple/dos/39633.txt

Apple QuickTime < 7.7.79.[01;31m[K80[m[K.95 - '.FPX' Parsing Memory Corruption (2) | multiple/dos/39634.txt

Apple QuickTime < 7.7.79.[01;31m[K80[m[K.95 - '.PSD' Parsing Memory Corruption | multiple/dos/39635.txt

Apple Safari 1.x - Cookie Directory Traversal | osx/remote/23[01;31m[K80[m[K0.txt

Apple Safari 6.0.1 for iOS 6.0 / Apple Mac OSX 10.7/8 - Heap Buffer Overflow | ios/remote/2[01;31m[K80[m[K81.txt

Apple Safari Web Browser 1.x - Infinite Array Sort Denial of Service | osx/dos/247[01;31m[K80[m[K.html

Apple Webkit - 'JSCallbackData' Universal Cross-Site Scripting | multiple/webapps/41[01;31m[K80[m[K0.html

Apple WebKit - 'RenderLayer' Use-After-Free | multiple/dos/41[01;31m[K80[m[K9.html

Apple Webkit - Universal Cross-Site Scripting by Accessing a Named Property from an Unloaded Window | multiple/webapps/41[01;31m[K80[m[K1.html

Apple WebKit 10.0.2 (12602.3.12.0.1) - 'disconnectSubframes' Universal Cross-Site Scripting | multiple/webapps/41[01;31m[K80[m[K2.html

Apple WebKit 10.0.2 (12602.3.12.0.1_ r210[01;31m[K80[m[K0) - 'constructJSReadableStreamDefaultReader' Type Confusion | multiple/webapps/41[01;31m[K80[m[K3.html

Apple WebKit 10.0.2 - HTMLInputElement Use-After-Free | multiple/dos/41[01;31m[K80[m[K7.html

AppServ Open Project 2.5.10 - 'appservlang' Cross-Site Scripting | php/webapps/31[01;31m[K80[m[K8.txt

AR Web Content Manager (AWCM) - 'cookie_gen.php' Arbitrary Cookie Generation |
php/webapps/3[01;31m[K80[m[K15.txt

ARD-9[01;31m[K80[m[K8 DVR Card Security Camera - Arbitrary Configuration Disclosure |
hardware/remote/9066.txt

ARD-9[01;31m[K80[m[K8 DVR Card Security Camera - GET Remote Denial of Service |
hardware/dos/9067.py

Aruba MC-[01;31m[K80[m[K0 Mobility Controller - Screens Directory HTML Injection |
multiple/remote/30771.txt

AShop Deluxe 4.5 - 'shipping.php' Cross-Site Scripting
| php/webapps/293[01;31m[K80[m[K.txt

ASMAX AR [01;31m[K80[m[K4 gu Web Management Console - Arbitrary Command Execution |
hardware/remote/8846.txt

ASP ActionCalendar 1.3 - Authentication Bypass
| asp/webapps/7[01;31m[K80[m[K7.txt

ASP Battle Blog - Database Disclosure
| asp/webapps/107[01;31m[K80[m[K.txt

ASP Download 1.03 - Arbitrary Change Administrator Account
| asp/webapps/57[01;31m[K80[m[K.txt

ASP-Nuke 2.0.7 - 'gotourl.asp' Open Redirect
| asp/webapps/325[01;31m[K80[m[K.txt

AspEmail v5.6.0.2 - Local Privilege Escalation
| windows/local/513[01;31m[K80[m[K.txt

ASPNuke 0.[01;31m[K80[m[K - 'article.asp' SQL Injection
| asp/webapps/1070.pl

ASPNuke 0.[01;31m[K80[m[K - 'Comments.asp' SQL Injection
| asp/webapps/25498.txt

ASPNuke 0.[01;31m[K80[m[K - 'comment_post.asp' SQL Injection
| asp/webapps/1071.pl

ASPNuke 0.[01;31m[K80[m[K - 'detail.asp' SQL Injection
| asp/webapps/25500.txt

ASPNuke 0.[01;31m[K80[m[K - 'forgot_password.asp?email' Cross-Site Scripting |
asp/webapps/25905.txt

```
ASPNuke 0.[01;31m[K80[m[K - 'Language_Select.asp' HTTP Response
Splitting                                                 |
asp/webapps/25907.txt

ASPNuke 0.[01;31m[K80[m[K - 'profile.asp' Cross-Site Scripting
| asp/webapps/25501.txt

ASPNuke 0.[01;31m[K80[m[K - 'register.asp' Multiple Cross-Site
Scripting Vulnerabilities                                  |
asp/webapps/25906.txt

ASPNuke 0.[01;31m[K80[m[K - 'register.asp' SQL Injection
| asp/webapps/2813.txt

ASPNuke 0.[01;31m[K80[m[K - 'Select.asp' Cross-Site Scripting
| asp/webapps/25502.txt

ASPSiteWare Project Reporter - SQL Injection
| asp/webapps/156[01;31m[K80[m[K.txt

Asterisk 1.8.4.1 - SIP 'REGISTER' Request User Enumeration
| linux/remote/35[01;31m[K80[m[K1.txt

AsusWRT Router < 3.0.0.4.3[01;31m[K80[m[K.7743 - LAN Remote Code
Execution                                                 |
hardware/remote/43881.txt

ASUSWRT RT-AC53 (3.0.0.4.3[01;31m[K80[m[K.6038) - Cross-Site Scripting
| hardware/webapps/41571.txt

ASUSWRT RT-AC53 (3.0.0.4.3[01;31m[K80[m[K.6038) - Remote Code Execution
| hardware/webapps/41573.txt

ASUSWRT RT-AC53 (3.0.0.4.3[01;31m[K80[m[K.6038) - Session Stealing
| hardware/webapps/41572.txt

AT Computing atsar_linux 1.4 - File Manipulation
| linux/local/19[01;31m[K80[m[K4.pl

atari[01;31m[K80[m[K0 - Local Privilege Escalation
| linux/local/657.c

Atlassian Jira Server Data Center 8.16.0 - Arbitrary File Read
| multiple/webapps/503[01;31m[K80[m[K.txt

Atmail WebMail - 'searchResultsTab5?filter' Reflected Cross-Site
Scripting                                  |
php/webapps/390[01;31m[K80[m[K.txt

Atomic Photo Album 1.0.2 - Multiple Vulnerabilities
| php/webapps/14[01;31m[K80[m[K1.txt
```

```
Atomic Photo Album 1.1.0pre4 - Insecure Cookie Handling
| php/webapps/65[01;31m[K80[m[K.txt

Atrium Software Mercur Mail Server 3.2 - Multiple Buffer Overflows (1)
| windows/dos/19[01;31m[K80[m[K6.c

Atrium Software Mercur Mail Server 3.2 - Multiple Buffer Overflows (2)
| windows/dos/19[01;31m[K80[m[K7.txt

Attendance and Payroll System v1.0 - Remote Code Execution (RCE)
| php/webapps/50[01;31m[K80[m[K1.py

Attendance and Payroll System v1.0 - SQLi Authentication Bypass
| php/webapps/50[01;31m[K80[m[K2.py

ATutor 1.5.x - '/admin/fix_content.php?submit' Cross-Site Scripting
| php/webapps/281[01;31m[K80[m[K.txt

ATutor 2.1 - 'tool_file' Local File Inclusion
| php/webapps/3[01;31m[K80[m[K40.txt

AuthPhp 1.0 - Authentication Bypass
| php/webapps/[01;31m[K80[m[K33.txt

AutoCAD DWG and DXF To PDF Converter 2.2 - Local Buffer Overflow
| windows/local/3[01;31m[K80[m[K87.pl

Avaya Aura Communication Manager 5.2 - Remote Code Execution
| hardware/webapps/4[01;31m[K80[m[K77.txt

AVideo Platform 8.1 - Cross Site Request Forgery (Password Reset)
| json/webapps/4[01;31m[K80[m[K03.txt

Aviosoft Digital TV Player Professional 1.x - Local Stack Buffer
Overflow                                  |
windows/local/1[01;31m[K80[m[K96.py

Avirt Gateway Suite 3.3 a/3.5 - Mail Server Buffer Overflow (1)
| windows/remote/195[01;31m[K80[m[K.txt

AWAuctionScript CMS - Multiple Remote Vulnerabilities
| php/webapps/3[01;31m[K80[m[K09.txt

AwesomeTemplateEngine 1 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/309[01;31m[K80[m[K.txt

AxisInternet VoIP Manager - Multiple Cross-Site Scripting
Vulnerabilities                                  |
cgi/webapps/37[01;31m[K80[m[K6.txt

Baby Katie Media VSReal and VScal 1.0 - 'myslideshow.php?title' Cross-
Site Scripting                        |
php/webapps/2[01;31m[K80[m[K00.txt
```

```
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)
| windows/remote/16[01;31m[K80[m[K6.rb

Bandersnatch 0.4 - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                                  |
php/webapps/30[01;31m[K80[m[K1.txt

BankTown ActiveX Control 1.4.2.51817/1.5.2.50209 - Remote Buffer
Overflow                                        |
windows/remote/27[01;31m[K80[m[K6.txt

Baran CMS 1.0 - 'Arbitrary '.ASP' File Upload / File Disclosure / SQL
Injection / Cross-Site Scripting / C |
asp/webapps/[01;31m[K80[m[K48.txt

Barracuda Load Balancer - 'realm' Cross-Site Scripting
| hardware/remote/32[01;31m[K80[m[K1.txt

Barracuda SSL VPN 6[01;31m[K80[m[K - 'returnTo' Open Redirection
| hardware/remote/38536.txt

Barracuda SSL VPN 6[01;31m[K80[m[KVx 2.3.3.193 - Multiple Script
Injection Vulnerabilities                                  |
hardware/webapps/26527.txt

bbScript 1.1.2.1 - 'id' Blind SQL Injection
| php/webapps/108[01;31m[K80[m[K.php

bcoos 1.0.13 - 'file' Local File Inclusion
| php/webapps/31[01;31m[K80[m[K6.txt

Beat Websites - 'id' SQL Injection
| php/webapps/3[01;31m[K80[m[K61.txt

Beauty Parlour Management System 1.0 - 'sername' SQL Injection
| php/webapps/495[01;31m[K80[m[K.txt

Bedita 3.5.1 - Cross-Site Scripting
| php/webapps/3[01;31m[K80[m[K51.txt

beLive 0.2.3 - 'arch.php?arch' Local File Inclusion
| php/webapps/86[01;31m[K80[m[K.txt

Belkin Bulldog Plus - Web Service Buffer Overflow (Metasploit)
| windows/remote/16[01;31m[K80[m[K4.rb

Best pos Management System v1.0 - Remote Code Execution (RCE) on File
Upload                                    |
php/webapps/512[01;31m[K80[m[K.txt

Best Way GEM Engine - Multiple Vulnerabilities
| windows/remote/339[01;31m[K80[m[K.txt
```

BestWebApp Dating Site Login Component - Multiple Field SQL Injections
| asp/webapps/290[01;31m[K80[m[K.txt

BigACE 2.7.5 - Arbitrary File Upload
| php/webapps/170[01;31m[K80[m[K.txt

BigDump 0.29b and 0.32b - Multiple Vulnerabilities
| php/webapps/3[01;31m[K80[m[K76.txt

Bilder Galerie 1.0 - 'index.php' Remote File Inclusion
| php/webapps/304[01;31m[K80[m[K.txt

Bitweaver 1.x/2.0 - '/search/index.php?highlight' SQL Injection
| php/webapps/308[01;31m[K80[m[K.txt

BlackBoard Learn 8.0 - 'keywordraw' Cross-Site Scripting
| cgi/webapps/35[01;31m[K80[m[K2.txt

BlazeVideo HDTV Player 2.1 - '.PLF' Local Buffer Overflow
| windows/local/28[01;31m[K80[m[K.c

Blog PixelMotion - 'sauvBase.php' Arbitrary Database Backup
| php/webapps/53[01;31m[K80[m[K.txt

Blog Torrent 0.[01;31m[K80[m[K - 'BTDownload.php' Cross-Site Scripting
| php/webapps/24[01;31m[K80[m[K3.txt

Bloggeruniverse 2.0 Beta - 'id' SQL Injection
| php/webapps/[01;31m[K80[m[K43.pl

blogit! - SQL Injection / File Disclosure / Cross-Site Scripting
| php/webapps/7[01;31m[K80[m[K6.txt

BlogWorx 1.0 - 'id' SQL Injection
| php/webapps/54[01;31m[K80[m[K.txt

BlogWrite 0.91 - Remote File Disclosure / SQL Injection
| php/webapps/[01;31m[K80[m[K53.pl

BloofoxCMS 0.3.4 - 'lang' Local File Inclusion
| php/webapps/75[01;31m[K80[m[K.txt

BloofoxCMS 0.3.5 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/3[01;31m[K80[m[K06.txt

Bloq 0.5.4 - '/files/mainfile.php?page[path]' Remote File Inclusion
| php/webapps/28[01;31m[K80[m[K2.txt

Bloq 0.5.4 - 'rdf.php?page[path]' Remote File Inclusion
| php/webapps/28[01;31m[K80[m[K1.txt

Bloq 0.5.4 - 'rss2.php?page[path]' Remote File Inclusion
| php/webapps/28[01;31m[K80[m[K0.txt

```
Blue Utopia - 'index.php' Local File Inclusion
| php/webapps/32[01;31m[K80[m[K6.txt

BlueBird Pre-Release - Authentication Bypass
| php/webapps/[01;31m[K80[m[K35.txt

BlueStacks 4.[01;31m[K80[m[K.0.1060 - Denial of Service (PoC)
| windows/dos/46893.py

BlueZone - '.zft' File Local Denial of Service
| windows/dos/1[01;31m[K80[m[K29.pl

BlueZone Desktop - Multiple Malformed Files Local Denial of Service
Vulnerabilities                         |
windows/dos/1[01;31m[K80[m[K30.pl

BM Classifieds 200[01;31m[K80[m[K409 - Multiple SQL Injections
| php/webapps/5223.txt

BMC Service Desk Express 10.2.1.95 - Multiple Vulnerabilities
| asp/webapps/26[01;31m[K80[m[K6.txt

BOOTP Turbo 2.0.1214 - 'BOOTP Turbo' Unquoted Service Path
| windows/local/4[01;31m[K80[m[K78.txt

Boxoft WAV to MP3 Converter - 'convert' Local Buffer Overflow
| windows/local/3[01;31m[K80[m[K35.pl

Broadcom Wi-Fi SoC - 'dhd_handle_swc_evt' Heap Overflow
| hardware/remote/41[01;31m[K80[m[K8.txt

Broadcom Wi-Fi SoC - Heap Overflow 'wlc_tdls_cal_mic_chk' Due to Large
RSN IE in TDLS Setup Confirm Frame  |
hardware/dos/41[01;31m[K80[m[K6.txt

Broadcom Wi-Fi SoC - TDLS Teardown Request Remote Heap Overflow
| hardware/remote/41[01;31m[K80[m[K5.txt

BroadWin Webaccess SCADA/HMI Client - Remote Code Execution
| windows/remote/1[01;31m[K80[m[K51.txt

BS.Player 2.34 Build 9[01;31m[K80[m[K - '.bsl' Local Buffer Overflow
(SEH)                                                 |
windows/local/8249.php

BST (BestShopPro) - 'nowosci.php' Multiple Vulnerabilities
| php/webapps/1[01;31m[K80[m[K63.txt

BtiTracker 1.3.x < 1.4.x - SQL Injection
| php/webapps/13[01;31m[K80[m[K7.py
```

```
Bugzilla - 'editflagtypes.cgi' Multiple Cross-Site Scripting
Vulnerabilities                                  |
cgi/webapps/38[01;31m[K80[m[K6.txt

Bugzilla 4.2 - Tabular Reports Cross-Site Scripting
| cgi/webapps/38[01;31m[K80[m[K7.txt

burnCMS 0.2 - 'root' Remote File Inclusion
| php/webapps/3[01;31m[K80[m[K9.txt

Burning Board 1.1.1 - 'URL' Manipulation
| php/webapps/213[01;31m[K80[m[K.php

BusinessSpace 1.2 - 'id' SQL Injection
| php/webapps/[01;31m[K80[m[K11.txt

Butterfly ORGanizer 2.0.0 - Arbitrary Delete (Category/Account)
| php/webapps/5[01;31m[K80[m[K0.pl

BWMeter 5.4.0 - '.csv' Denial of Service
| windows/dos/161[01;31m[K80[m[K.py

Bytes interactive Web shopper 1.0/2.0 - Directory Traversal
| cgi/remote/202[01;31m[K80[m[K.txt

C.J. Steele Tattle - Remote Command Execution
| linux/remote/25[01;31m[K80[m[K2.txt

C4B XPhone UC Web 4.1.890S R1 - Cross-Site Scripting
| asp/webapps/18[01;31m[K80[m[K2.txt

CA iTechnology iGateway - Debug Mode Buffer Overflow (Metasploit)
| windows/remote/16[01;31m[K80[m[K1.rb

CA Unified Infrastructure Management Nimsoft 7.[01;31m[K80[m[K - Remote
Buffer Overflow                                  |
windows/remote/48156.c

Cacti Superlinks Plugin 1.4-2 - SQL Injection
| php/webapps/33[01;31m[K80[m[K9.txt

CadeNix - SQL Injection
| php/webapps/74[01;31m[K80[m[K.txt

CafeEngine - 'catid' SQL Injection
| php/webapps/[01;31m[K80[m[K02.txt

Calendarix 0.8.200[01;31m[K80[m[K[01;31m[K80[m[K8 - Multiple Cross-Site
Scripting / SQL Injections                                  |
php/webapps/35737.txt

Calibre E-Book Reader - Local Privilege Escalation (1)
| linux/local/1[01;31m[K80[m[K64.sh
```

```
Calibre E-Book Reader - Local Privilege Escalation (2)
| linux/local/1[01;31m[K80[m[K71.sh

Calibre E-Book Reader - Local Privilege Escalation (3)
| linux/local/1[01;31m[K80[m[K86.c

Calibre E-Book Reader - Race Condition Privilege Escalation
| linux/local/1[01;31m[K80[m[K72.sh

CaLogic Calendars 1.2.2 - 'CLPath' Remote File Inclusion
| php/webapps/1[01;31m[K80[m[K9.txt

CAM UnZip 5.1 - .'ZIP' File Directory Traversal
| windows/local/396[01;31m[K80[m[K.txt

Campsite 2.6.1 - 'IPAccess.php?g_documentRoot' Remote File Inclusion
| php/webapps/299[01;31m[K80[m[K.txt

Car Portal CMS 3.0 - Multiple Vulnerabilities
| php/webapps/18[01;31m[K80[m[K1.txt

CarLine Forum Russian Board 4.2 - 'search.php?text_poisk' Cross-Site
Scripting                                |
php/webapps/258[01;31m[K80[m[K.txt

CaupoShop Pro (2.x < 3.70) Classic 3.01 - Local File Inclusion
| php/webapps/1[01;31m[K80[m[K66.txt

CCextractor 0.[01;31m[K80[m[K - Crash (PoC)
| linux/dos/39873.py

CCMS 3.1 Demo - SQL Injection
| php/webapps/4[01;31m[K80[m[K9.py

Centos Web Panel 0.9.8.4[01;31m[K80[m[K - Multiple Vulnerabilities
| php/webapps/45610.txt

CentOS Web Panel 0.9.8.793 (Free) / v0.9.8.753 (Pro) /
0.9.8.[01;31m[K80[m[K7 (Pro) - Domain Field (Add DNS Zone) Cross |
linux/webapps/46784.txt

Cerb 7.0.3 - Cross-Site Request Forgery
| php/webapps/3[01;31m[K80[m[K74.txt

Cerberus Helpdesk 0.97.3/2.6.1 - Multiple Cross-Site Scripting
Vulnerabilities                          |
php/webapps/25[01;31m[K80[m[K3.txt

CEScripts (Multiple Scripts) - Cross-Site Scripting
| php/webapps/2[01;31m[K80[m[K17.txt

cFTP 0.1 - 'r[01;31m[K80[m[K' Arbitrary File Upload
| php/webapps/17584.php
```

```
Chaussette 0[01;31m[K80[m[K706 - '_BASE' Remote File Inclusion
| php/webapps/2169.txt

Check Point Software Firewall-1 3.0/1 4.0 / Cisco PIX Firewall 4.x/5.x
- 'ALG' Client                        |
multiple/remote/19[01;31m[K80[m[K0.c

CheckPoint Endpoint Security Client/ZoneAlarm
15.4.062.17[01;31m[K80[m[K2 - Privilege Escalation
| windows/local/47471.txt

Chipmunk Forum - 'recommend.php?ID' Cross-Site Scripting
| php/webapps/263[01;31m[K80[m[K.txt

Chipmunk Forums - SQL Injection
| php/webapps/[01;31m[K80[m[K9.txt

CHIYU BF430 TCP IP Converter - Stored Cross-Site Scripting
| cgi/webapps/4[01;31m[K80[m[K40.txt

Chrome V8 - 'TranslatedState::MaterializeCapturedObjectAt' Type
Confusion                                |
multiple/dos/441[01;31m[K80[m[K.js

Chupix CMS Contact Module 0.1 - 'index.php' Multiple Local File
Inclusions                               |
php/webapps/321[01;31m[K80[m[K.txt

CIScan 1.00 - Hostname/IP Field Overwrite (SEH) (PoC)
| windows/dos/39[01;31m[K80[m[K2.py

Cisco AnyConnect 3.1.0[01;31m[K80[m[K09 - Local Privilege Escalation
(via DMG Install Script)                          | osx/local/38303.c

Cisco AnyConnect Secure Mobility Client 3.1.0[01;31m[K80[m[K09 - Local
Privilege Escalation                             |
windows/local/38289.txt

Cisco CallManager 3.x/4.x - 'Web Interface
'ccmadmin/phonelist.asp?Pattern' Cross-Site Scripting          |
asp/webapps/2[01;31m[K80[m[K61.txt

Cisco CallManager 3.x/4.x - 'Web Interface 'ccmuser/logon.asp' Cross-
Site Scripting                          |
asp/webapps/2[01;31m[K80[m[K62.txt

Cisco Data Center Network Manager 11.2 - Remote Code Execution
| java/webapps/4[01;31m[K80[m[K18.py

Cisco Data Center Network Manager 11.2.1 - 'getVmHostData' SQL
Injection                                 |
java/webapps/4[01;31m[K80[m[K19.py
```

```
Cisco Data Center Network Manager 11.2.1 - 'LanFabricImpl' Command
Injection                                  |
java/webapps/4[01;31m[K80[m[K20.py

Cisco Secure ACS 2.3 - 'LoginProxy.cgi' Cross-Site Scripting
| unix/remote/2[01;31m[K80[m[K30.txt

Cisco Unified Operations Manager 8.5 - Common Services Device Center
Cross-Site Scripting                   |
hardware/remote/357[01;31m[K80[m[K.txt

Cisco VPN 5000 Client - Buffer Overrun (1)
| unix/local/21[01;31m[K80[m[K5.c

Cisco VPN 5000 Client - Buffer Overrun (2)
| unix/local/21[01;31m[K80[m[K6.c

CitectSCADA/CitectFacilities ODBC - Remote Buffer Overflow (Metasploit)
| windows/remote/163[01;31m[K80[m[K.rb

Citrix Access Gateway - Command Injection
| linux/remote/15[01;31m[K80[m[K6.txt

Citrix Netscaler SOAP Handler - Remote Code Execution (Metasploit)
| bsd/remote/351[01;31m[K80[m[K.rb

Clain_TIger_CMS - Cross-Site Request Forgery
| php/webapps/117[01;31m[K80[m[K.html

ClanSphere 2011.0 - Local File Inclusion / Arbitrary File Upload
| php/webapps/356[01;31m[K80[m[K.txt

ClickAuction - Authentication Bypass
| php/webapps/78[01;31m[K80[m[K.txt

Client Details System 1.0 - SQL Injection
| php/webapps/518[01;31m[K80[m[K.txt

Cline Communications - Multiple SQL Injections
| php/webapps/2[01;31m[K80[m[K57.txt

Clipbucket 1.7 - 'dwnld.php' Directory Traversal
| php/webapps/32[01;31m[K80[m[K2.txt

Cloudflare WARP 1.4 - Unquoted Service Path
| windows/local/50[01;31m[K80[m[K5.txt

CMS Faethon 1.3.2 - Multiple Remote File Inclusions
| php/webapps/2[01;31m[K80[m[K47.txt

CMS mini 0.2.2 - Local File Inclusion
| php/webapps/1[01;31m[K80[m[K01.txt
```

```
CMScore - SQL Injection
| php/webapps/[01;31m[K80[m[K8.txt

CMScout - Cross-Site Scripting / HTML Injection
| php/webapps/12[01;31m[K80[m[K6.txt

CmsFaethon 2.2.0 - 'item' SQL Injection
| php/webapps/[01;31m[K80[m[K54.pl

CMSsite 1.0 - Multiple Cross-Site Request Forgery
| php/webapps/464[01;31m[K80[m[K.txt

CodeBlocks 12.11 (OSX) - Crash (PoC)
| osx/dos/25[01;31m[K80[m[K9.py

CodetoSell ViArt Shop Enterprise 2.1.6 - 'news_view.php' Multiple
Cross-Site Scripting Vulnerabilities     |
php/webapps/255[01;31m[K80[m[K.txt

Cogent DataHub - Command Injection (Metasploit)
| windows/remote/338[01;31m[K80[m[K.rb

Comdev eCommerce 3.0 - 'WCE.download.php' Directory Traversal
| php/webapps/260[01;31m[K80[m[K.txt

comments-like-dislike < 1.2.0 - Authenticated (Subscriber+) Plugin
Setting Reset                            |
php/webapps/51[01;31m[K80[m[K9.py

Computer Software Manufaktur Alibaba 2.0 - Denial of Service
| windows/dos/200[01;31m[K80[m[K.c

COMTREND CT-507 IT ADSL Router - 'scvrtsrv.cmd' Cross-Site Scripting
| hardware/remote/335[01;31m[K80[m[K.txt

Confixx 3.0/3.1 - 'FTP_index.php' Cross-Site Scripting
| php/webapps/2[01;31m[K80[m[K23.txt

CoolPlayer Portable 2.19.2 - Local Buffer Overflow (ASLR Bypass) (1)
| windows/local/177[01;31m[K80[m[K.py

CoolShot E-Lite POS 1.0 - Login SQL Injection
| php/webapps/30[01;31m[K80[m[K3.txt

coppermine 1.5.18 - Multiple Vulnerabilities
| php/webapps/186[01;31m[K80[m[K.txt

Core FTP Server 1.2 - Local Buffer Overflow
| windows/local/394[01;31m[K80[m[K.py

Corel PDF Fusion - Local Stack Buffer Overflow (Metasploit)
| windows/local/26[01;31m[K80[m[K5.rb
```

```
Cornerstone CMS - SQL Injection
| php/webapps/139[01;31m[K80[m[K.txt

Coship Wireless Router 4.0.0.48 / 4.0.0.40 / 5.0.0.54 / 5.0.0.55 /
10.0.0.49 - Unauthenticated Admin Passw |
hardware/webapps/461[01;31m[K80[m[K.html

CoSoSys Endpoint Protector - Predictable Password Generation
| hardware/remote/37[01;31m[K80[m[K3.txt

Cotonti 0.9.2 - Multiple SQL Injections
| php/webapps/35[01;31m[K80[m[K3.txt

COWON America jetCast 2.0.4.1109 - '.mp3' Local Overflow
| windows/local/87[01;31m[K80[m[K.php

cPanel 10.9.1 - 'Resname' Cross-Site Scripting
| php/webapps/303[01;31m[K80[m[K.txt

cPanel 11.21 - 'wwwact' Privilege Escalation
| php/webapps/31[01;31m[K80[m[K7.txt

cPanel 5/6/7/8/9 - 'dir' Cross-Site Scripting
| cgi/webapps/23[01;31m[K80[m[K6.txt

cPanel 5/6/7/8/9 - Login Script Remote Command Execution
| cgi/webapps/23[01;31m[K80[m[K7.txt

cPanel 5/6/7/8/9 - Resetpass Remote Command Execution
| cgi/remote/23[01;31m[K80[m[K4.txt

CreaCMS - '/fonctions/get_liste_langue.php?cfg[base_uri_admin]' Remote
File Inclusion                        |
php/webapps/320[01;31m[K80[m[K.txt

Creato Script - SQL Injection
| php/webapps/12[01;31m[K80[m[K7.txt

Crimson Editor - Overwrite (SEH)
| windows/dos/11[01;31m[K80[m[K3.txt

CrossWind CyberScheduler 2.1 - websyncd Remote Buffer Overflow
| cgi/remote/207[01;31m[K80[m[K.c

CrowdStrike Falcon AGENT  6.44.15[01;31m[K80[m[K6  - Uninstall without
Installation Token                                  |
windows/local/51146.ps1

Crypttech CryptoLog - Remote Code Execution (Metasploit)
| python/remote/419[01;31m[K80[m[K.rb

Cuckoo Clock v5.0 - Buffer Overflow
| windows/local/4[01;31m[K80[m[K87.py
```

```
CuteNews 2.1.2 - Remote Code Execution
| php/webapps/48[01;31m[K80[m[K0.py

CVSWeb Developer CVSWeb 1.[01;31m[K80[m[K - Insecure Perl 'open' Code
Execution                                          |
unix/local/20073.txt

Cyberoam Firewall CR500iNG-XP 10.6.2 MR-1 - Blind SQL Injection
| hardware/webapps/3[01;31m[K80[m[K34.txt

Cyclope Internet Filtering Proxy 4.0 - 'CEPMServer.exe' Denial of
Service (PoC)                              |
windows/dos/1[01;31m[K80[m[K17.py

Cyclope Internet Filtering Proxy 4.0 - Persistent Cross-Site Scripting
| windows/webapps/1[01;31m[K80[m[K13.py

CyrixMED 1.4 - 'index.php' Cross-Site Scripting
| php/webapps/317[01;31m[K80[m[K.txt

Cytel Studio 9.0 - '.CY3' Local Stack Buffer Overflow (Metasploit)
| windows/local/1[01;31m[K80[m[K27.rb

D-Link Devices - Unauthenticated Remote Command Execution in ssdpcgi
(Metasploit)                               |
linux_mips/remote/4[01;31m[K80[m[K37.rb

D-Link DIR-8[01;31m[K80[m[KL - Multiple Buffer Overflow Vulnerabilities
| hardware/remote/38725.txt

D-Link DIR-Series Routers - HNAP Login Stack Buffer Overflow
(Metasploit)                                       |
multiple/remote/40[01;31m[K80[m[K5.rb

D-Link DSL-27[01;31m[K80[m[KB DLink_1.01.14 - Remote DNS Change
| hardware/webapps/37237.txt

dacio's CMS 1.08 - Cross-Site Scripting / SQL Injection / File
Disclosure                                         |
php/webapps/[01;31m[K80[m[K42.txt

Daemon Tools Lite - 'mfc[01;31m[K80[m[Kloc.dll' DLL Hijacking
| windows/local/14791.c

darryl burgdorf weblibs 1.0 - Directory Traversal
| php/webapps/24[01;31m[K80[m[K6.txt

Data Center Audit 2.6.2 - 'username' SQL Injection
| php/webapps/45[01;31m[K80[m[K7.txt

DataTaker DT[01;31m[K80[m[K dEX 1.50.012 - Information Disclosure
| hardware/webapps/42313.txt
```

```
datawizard webxq 2.1.204 - Directory Traversal
| multiple/remote/20[01;31m[K80[m[K7.txt

Datecomm 1.1 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/2[01;31m[K80[m[K60.txt

Dating Agent 4.7.1 - Multiple Input Validation Vulnerabilities
| php/webapps/2[01;31m[K80[m[K97.txt

davfs2 1.4.6/1.4.7 - Local Privilege Escalation
| linux/local/28[01;31m[K80[m[K6.txt

DB4Web 3.4/3.6 - Connection Proxy
| multiple/remote/21[01;31m[K80[m[K1.txt

DB4Web 3.4/3.6 - File Disclosure
| multiple/remote/21[01;31m[K80[m[K0.txt

DBPower C300 HD Camera - Remote Configuration Disclosure
| hardware/webapps/4[01;31m[K80[m[K95.pl

DCForum - 'auth_user_file.txt' File Multiple Information Disclosure
Vulnerabilities                         |
php/webapps/3[01;31m[K80[m[K07.txt

Debian suidmanager 0.18 - Command Execution
| linux/local/190[01;31m[K80[m[K.txt

DelphiTurk FTP 1.0 - Passwords to Local Users
| windows/local/[01;31m[K80[m[K3.c

Delta Controls enteliTOUCH 3.40.3935 - Cookie User Password Disclosure
| hardware/remote/508[01;31m[K80[m[K.txt

Den Dating 9.01 - 'txtlookgender' SQL Injection
| php/webapps/[01;31m[K80[m[K44.txt

DHCP Turbo 4.61298 - 'DHCP Turbo 4' Unquoted Service Path
| windows/local/4[01;31m[K80[m[K[01;31m[K80[m[K.txt

Dicshunary 0.1a - 'check_status.php' Remote File Inclusion
| php/webapps/2[01;31m[K80[m[K8.txt

Diesel Job Site 1.4 - Multiple Vulnerabilities
| php/webapps/10[01;31m[K80[m[K5.txt

Digital Hive 2.0 - 'base_include.php' Local File Inclusion
| php/webapps/31[01;31m[K80[m[K4.txt

Disc ORGanizer (DORG) - Multiple Vulnerabilities
| php/webapps/395[01;31m[K80[m[K.txt
```

```
Disconnect.me Mac OSX Client 2.0 - Local Privilege Escalation
| osx/local/3[01;31m[K80[m[K89.txt

Disk Savvy Enterprise 12.3.18 - Unquoted Service Path
| windows/local/4[01;31m[K80[m[K49.txt

Disk Sorter Enterprise 12.4.16 - 'Disk Sorter Enterprise' Unquoted
Service Path                          |
windows/local/4[01;31m[K80[m[K48.txt

DIY CMS 1.0 Poll - Multiple Vulnerabilities
| php/webapps/18[01;31m[K80[m[K4.txt

DLINK DCS-5020L - Remote Code Execution (PoC)
| hardware/webapps/445[01;31m[K80[m[K.txt

dl_stats - Multiple Vulnerabilities
| php/webapps/122[01;31m[K80[m[K.txt

DmxReady Faqs Manager 1.2 - SQL Injection
| asp/webapps/174[01;31m[K80[m[K.txt

Docker 0.11 - VMM-Container Breakout
| linux/local/33[01;31m[K80[m[K8.c

Dokeos 1.6.5 - 'courseLog.php?scormcontopen' SQL Injection
| php/webapps/39[01;31m[K80[m[K.pl

Dolibarr ERP/CRM 3.2.0 < Alpha - File Inclusion
| php/webapps/184[01;31m[K80[m[K.txt

Dolibarr ERP/CRM 7.0.0 - (Authenticated) SQL Injection
| php/webapps/44[01;31m[K80[m[K5.txt

DomPHP 0.81 - Remote Add Administrator
| php/webapps/48[01;31m[K80[m[K.php

Dota 2 7.23f - Denial of Service (PoC)
| windows/dos/4[01;31m[K80[m[K31.txt

dotProject 2.1.x - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities                              |
php/webapps/3[01;31m[K80[m[K43.txt

dotProject 2.1.x - 'index.php' Multiple SQL Injections
| php/webapps/3[01;31m[K80[m[K42.txt

dotWidget for articles 2.0 - '/admin/articles.php' Multiple Remote File
Inclusions                          | php/webapps/2[01;31m[K80[m[K42.txt

dotWidget for articles 2.0 - '/admin/authors.php' Multiple Remote File
Inclusions                           |
php/webapps/2[01;31m[K80[m[K41.txt
```

dotWidget for articles 2.0 - '/admin/categories.php' Multiple Remote File Inclusions | php/webapps/2[01;31m[K80[m[K45.txt

dotWidget for articles 2.0 - '/admin/editconfig.php' Multiple Remote File Inclusions | php/webapps/2[01;31m[K80[m[K46.txt

dotWidget for articles 2.0 - '/admin/index.php' Multiple Remote File Inclusions | php/webapps/2[01;31m[K80[m[K43.txt

dotWidget for articles 2.0 - 'showarticle.php?file_path' Remote File Inclusion | php/webapps/2[01;31m[K80[m[K40.txt

dotWidget for articles 2.0 - 'showcatpicks.php?file_path' Remote File Inclusion | php/webapps/2[01;31m[K80[m[K39.txt

DoubleSpeak 0.1 - Multiple Remote File Inclusions
| php/webapps/2[01;31m[K80[m[K16.txt

Drake CMS 0.3.7 - '404.php' Local File Inclusion
| php/webapps/29[01;31m[K80[m[K5.txt

DreamBox DM[01;31m[K80[m[K0 - 'file' Local File Disclosure
| hardware/webapps/36286.txt

DreamBox DM[01;31m[K80[m[K0 - Arbitrary File Download
| hardware/remote/17422.txt

DreamBox DM[01;31m[K80[m[K0 1.5rc1 - File Disclosure
| hardware/remote/1[01;31m[K80[m[K79.pl

dreamMail e-mail client 4.6.9.2 - Persistent Cross-Site Scripting
| windows/remote/27[01;31m[K80[m[K5.py

DUportal Pro 3.4 - 'cat.asp' Multiple SQL Injections
| asp/webapps/254[01;31m[K80[m[K.txt

DVD Photo Slideshow Professional 8.07 - 'Key' Buffer Overflow
| windows/local/4[01;31m[K80[m[K41.py

DVD Photo Slideshow Professional 8.07 - 'Name' Buffer Overflow
| windows/local/4[01;31m[K80[m[K46.py

DVD X Player 5.5 Pro - Local Overflow (SEH + ASLR + DEP Bypass)
| windows/local/17[01;31m[K80[m[K3.php

E-Pay - Remote File Inclusion
| php/webapps/106[01;31m[K80[m[K.txt

```
E-Sic Software livre CMS - Autentication Bypass
| php/webapps/429[01;31m[K80[m[K.txt

E-Smart Cart - 'productsofcat.asp' SQL Injection
| asp/webapps/5[01;31m[K80[m[K5.txt

e107 0.7.5 - 'search.php' Cross-Site Scripting
| php/webapps/2[01;31m[K80[m[K63.txt

e107 0.7.5 - 'Subject' HTML Injection
| php/webapps/2[01;31m[K80[m[K78.txt

e107 < 2.1.4 - 'keyword' Blind SQL Injection
| php/webapps/415[01;31m[K80[m[K.pl

ea-gBook 0.1 - Remote Command Execution / Remote File Inclusion
| php/webapps/[01;31m[K80[m[K52.pl

Easy Chat Server 3.1 - 'message' Denial of Service (PoC)
| windows/dos/46[01;31m[K80[m[K6.py

Easy File Management Web Server 5.6 - 'USERID' Remote Buffer Overflow
| windows/remote/37[01;31m[K80[m[K8.py

Easy-Clanpage 2.2 - Multiple SQL Injections /
| php/webapps/119[01;31m[K80[m[K.txt

Easy-Clanpage 3.0b1 - 'section' Local File Inclusion
| php/webapps/5[01;31m[K80[m[K1.txt

Easy2Pilot 7 - Cross-Site Request Forgery (Add User)
| php/webapps/4[01;31m[K80[m[K99.txt

EasyPHP Devserver 16.1.1 - Cross-Site Request Forgery / Remote Command
Execution                          |
php/webapps/40[01;31m[K80[m[K9.txt

ecava IntegraXor 3.6.4000.0 - Directory Traversal
| windows/remote/15[01;31m[K80[m[K2.txt

Eclipse Equinoxe OSGi Console - Command Execution (Metasploit)
| multiple/remote/442[01;31m[K80[m[K.rb

ECOA Building Automation System - Configuration Download Information
Disclosure                           |
hardware/webapps/502[01;31m[K80[m[K.txt

Ecommerce Systempay 1.0 - Production KEY Brute Force
| php/webapps/4[01;31m[K80[m[K17.php

Edimax BR6228nS/BR6228nC - Multiple Vulnerabilities
| hardware/webapps/3[01;31m[K80[m[K56.txt
```

```
Edimax PS-1206MF - Web Admin Authentication Bypass
| hardware/webapps/3[01;31m[K80[m[K29.txt

eDisplay Personal FTP Server 1.0.0 - Denial of Service (PoC)
| windows/dos/11[01;31m[K80[m[K9.py

Eduha Meeting - 'index.php' Arbitrary File Upload
| php/webapps/2[01;31m[K80[m[K58.txt

eFAQ - Authentication Bypass
| asp/webapps/7[01;31m[K80[m[K0.txt

eFront 3.6.10 (build 11944) - Multiple Vulnerabilities
| php/webapps/1[01;31m[K80[m[K36.txt

eFront 3.6.14 (build 1[01;31m[K80[m[K12) - Multiple Persistent Cross-
Site Scripting Vulnerabilities                     |
php/webapps/30213.txt

eIQnetworks License Manager - Remote Buffer Overflow (multi) (1)
| windows/remote/20[01;31m[K80[m[K.pl

ELAN Smart-Pad 11.10.15.1 - 'ETDService' Unquoted Service Path
| windows/local/4[01;31m[K80[m[K09.txt

Elastix - 'page' Cross-Site Scripting
| php/webapps/3[01;31m[K80[m[K78.py

Elastix < 2.5 - PHP Code Injection
| php/webapps/3[01;31m[K80[m[K91.php

ELOG 2.5.6 - Remote Shell
| multiple/remote/[01;31m[K80[m[K5.c

eM Client e-mail client 5.0.1[01;31m[K80[m[K25.0 - Persistent Cross-
Site Scripting                                      |
windows/remote/28183.py

EMC Captiva QuickScan Pro 4.6 SP1 and EMC Documentum ApllicationXtender
Desktop 5.4 (keyhelp.ocx 1.2.312)  |
windows/remote/9[01;31m[K80[m[K3.html

Emerson PAC Machine Edition 9.[01;31m[K80[m[K Build 8695 -
'TrapiServer' Unquoted Service Path                          |
windows/local/50745.txt

Employee Management System v1 - 'email' SQL Injection
| php/webapps/51[01;31m[K80[m[K3.txt

Employee Record System 1.0 - Multiple Stored XSS
| php/webapps/492[01;31m[K80[m[K.txt
```

```
EMS Master Calendar < 8.0.0.201[01;31m[K80[m[K520 - Cross-Site
Scripting                                                    |
aspx/webapps/44831.txt

Emumail EMU Webmail 5.2.7 - nit.emu Information Disclosure
| cgi/webapps/23[01;31m[K80[m[K9.txt

EncapsGallery 1.11.2 - 'catalog_watermark.php?file' Cross-Site
Scripting                                      |
php/webapps/313[01;31m[K80[m[K.txt

Endian Firewall - Password Change Command Injection (Metasploit)
| linux/remote/3[01;31m[K80[m[K96.rb

eNdonesia CMS 8.4 - Local File Inclusion
| php/webapps/98[01;31m[K80[m[K.txt

Enlightenment v0.25.3 - Privilege escalation
| linux/local/511[01;31m[K80[m[K.txt

Enomaly ECP / Enomalism < 2.2.1 - Multiple Local Vulnerabilities
| multiple/local/[01;31m[K80[m[K67.txt

Enterasys SSR[01;31m[K80[m[K00 SmartSwitch - Port Scan Denial of
Service                                                      |
hardware/dos/21791.txt

EPSON EasyMP Network Projection 2.81 - 'EMP_NSWLSV' Unquoted Service
Path                                    |
windows/local/4[01;31m[K80[m[K69.txt

eReservations - Authentication Bypass
| asp/webapps/7[01;31m[K80[m[K1.txt

EsForum 3.0 - 'forum.php?idsalon' SQL Injection
| php/webapps/3[01;31m[K80[m[K6.txt

eshtery CMS - SQL Injection
| asp/webapps/149[01;31m[K80[m[K.txt

eSignal and eSignal Pro 10.6.2425.1208 - File Parsing Buffer Overflow
in QUO (Metasploit)                    |
windows/local/178[01;31m[K80[m[K.rb

ESMI PayPal StoreFront 1.7 - Cross-Site Scripting
| php/webapps/252[01;31m[K80[m[K.txt

ESRI ArcGIS for Server - 'where' SQL Injection
| multiple/webapps/3[01;31m[K80[m[K16.txt

EternalMart Guestbook 1.10 - '/admin/auth.php' Remote File Inclusion
| php/webapps/29[01;31m[K80[m[K.txt
```

Ettercap 0.8.0 < 0.8.1 - Multiple Denial of Service Vulnerabilities
| linux/dos/355[01;31m[K80[m[K.rb

Eudora Qualcomm WorldMail 3.0 - 'IMAPd' Remote Overflow
| windows/remote/13[01;31m[K80[m[K.py

eWON Flexy - Authentication Bypass
| hardware/webapps/473[01;31m[K80[m[K.py

ExaGrid - Known SSH Key and Default Password (Metasploit)
| linux/remote/416[01;31m[K80[m[K.rb

Excite for Web Servers 1.1 - Administrative Password
| cgi/remote/20[01;31m[K80[m[K9.html

Exim ESMTP 4.[01;31m[K80[m[K - glibc gethostbyname Denial of Service
| linux/dos/35951.py

eXPert PDF 7.0.8[01;31m[K80[m[K.0 - '.pj' Heap Buffer Overflow
| windows/dos/35656.pl

eXPert PDF Batch Creator 7.0.8[01;31m[K80[m[K.0 - Denial of Service
| windows/dos/35502.pl

ExpertGPS 6.38 - XML External Entity Injection
| xml/webapps/4[01;31m[K80[m[K26.txt

Ext 1.0 - 'feed-proxy.php?feed' Remote File Disclosure
| php/webapps/3[01;31m[K80[m[K0.txt

EyesOfNetwork 5.1 - Authenticated Remote Command Execution
| php/webapps/472[01;31m[K80[m[K.py

EyesOfNetwork 5.3 - Remote Code Execution
| php/webapps/4[01;31m[K80[m[K25.txt

EZDatabaseRemote 2.0 - PHP Script Code Execution
| php/webapps/270[01;31m[K80[m[K.txt

eZip Wizard 3.0 - Local Stack Buffer Overflow (PoC) (SEH)
| windows/dos/81[01;31m[K80[m[K.c

ezpack 4.2b2 - Cross-Site Scripting / SQL Injection
| php/webapps/76[01;31m[K80[m[K.txt

Facebook Clone Script 1.0 - 'id' / 'send' SQL Injection
| php/webapps/432[01;31m[K80[m[K.txt

Facebook Clone Script 1.0.5 - Cross-Site Request Forgery
| php/webapps/44[01;31m[K80[m[K0.txt

Falt4 CMS RC4 - 'FCKeditor' Arbitrary File Upload
| php/webapps/[01;31m[K80[m[K60.php

```
Fast Click SQL Lite 1.1.2/1.1.3 - 'show.php' Remote File Inclusion
| php/webapps/27[01;31m[K80[m[K7.txt

feedDemon 2.7 - OPML Outline Tag Buffer Overflow
| windows/local/[01;31m[K80[m[K10.pl

Feng Office - Security Bypass / HTML Injection
| php/webapps/3[01;31m[K80[m[K44.txt

File117 - Multiple Remote File Inclusions
| php/webapps/298[01;31m[K80[m[K.txt

FileExecutive 1 - Multiple Vulnerabilities
| aix/webapps/115[01;31m[K80[m[K.txt

FileZilla FTP Client 3.17.0.0 - Unquoted Path Privilege Escalation
| windows/local/39[01;31m[K80[m[K3.txt

fims File Management System 1.2.1a - Multiple Vulnerabilities
| php/webapps/1[01;31m[K80[m[K03.txt

Firebird 1.0 - GDS_Inet_Server Interbase Environment Variable Buffer
Overflow                                |
freebsd/local/225[01;31m[K80[m[K.c

FireConfig 0.5 - 'dl.php' Remote File Disclosure
| php/webapps/45[01;31m[K80[m[K.txt

FireEye Appliance - Unauthorized File Disclosure
| php/webapps/3[01;31m[K80[m[K90.txt

Firefly 1.1.01 - 'doc_root' Remote File Inclusion
| php/webapps/3[01;31m[K80[m[K5.txt

Firepack - '/admin/ref.php' Remote Code Execution
| php/webapps/[01;31m[K80[m[K75.pl

Five Star Review Script - 'index2.php?sort' Cross-Site Scripting
| php/webapps/2[01;31m[K80[m[K09.txt

Five Star Review Script - 'report.php?item_id' Cross-Site Scripting
| php/webapps/2[01;31m[K80[m[K10.txt

Flash Image Gallery 1.1 - Arbitrary Configuration File Disclosure
| php/webapps/8[01;31m[K80[m[K5.txt

FlatNuke 2.5.x - 'help.php' Multiple Cross-Site Scripting
Vulnerabilities                                 |
php/webapps/25[01;31m[K80[m[K0.txt

FlatNuke 2.5.x - 'referer.php' Crafted Referer Arbitrary PHP Code
Execution                                  |
php/webapps/25[01;31m[K80[m[K1.php
```

```
Flatpress 0.[01;31m[K80[m[K4 - Multiple Cross-Site Scripting
Vulnerabilities                                              |
php/webapps/32421.html

Flatpress 0.[01;31m[K80[m[K4 < 0.812.1 - Local File Inclusion
| php/webapps/9[01;31m[K80[m[K1.txt

FLEX 10[01;31m[K80[m[K < 1085 Web 1.6.0 - Denial of Service
| android/dos/51438.py

FlexCMS 2.5 - 'catId' SQL Injection
| php/webapps/[01;31m[K80[m[K18.txt

FLIP 0.9.0.1029 - 'text.php?name' Cross-Site Scripting
| php/webapps/268[01;31m[K80[m[K.txt

Fluorine CMS 0.1 rc 1 - File Disclosure / SQL Injection / Command
Execution                                    |
php/webapps/[01;31m[K80[m[K36.pl

Foing 0.x - Remote File Inclusion
| php/webapps/2[01;31m[K80[m[K12.txt

FooSun - 'Api_Response.asp' SQL Injection
| asp/webapps/30[01;31m[K80[m[K0.html

Forcepoint WebSecurity 8.5 - Reflective Cross-Site Scripting
| multiple/webapps/4[01;31m[K80[m[K29.txt

Forescout CounterACT - 'a' Open Redirection
| multiple/webapps/3[01;31m[K80[m[K62.txt

Fork CMS - 'js.php' Local File Inclusion
| php/webapps/384[01;31m[K80[m[K.txt

FOSS Gallery Public 1.0 - Arbitrary File Upload (PoC)
| php/webapps/66[01;31m[K80[m[K.txt

Foswiki MAKETEXT - Remote Command Execution (Metasploit)
| unix/remote/235[01;31m[K80[m[K.rb

Foxit PDF Reader 11.0 - Unquoted Service Path
| windows/local/50[01;31m[K80[m[K7.txt

Foxit Reader 3.2.1.0401 - Denial of Service
| windows/dos/120[01;31m[K80[m[K.txt

Franklin Fueling Systems Colibri Controller Module
1.8.19.85[01;31m[K80[m[K - Local File Inclusion (LFI)                |
linux/remote/50861.txt

Franklin Fueling TS-550 evo 2.0.0.6833 - Multiple Vulnerabilities
| hardware/webapps/311[01;31m[K80[m[K.txt
```

```
Frappe Framework (ERPNext) 13.4.0 - Remote Code Execution
(Authenticated)                                    |
python/webapps/515[01;31m[K80[m[K.txt

Free Arcade Script 1.0 - Local File Inclusion Command Execution
| php/webapps/[01;31m[K80[m[K94.pl

Free CD to MP3 Converter 3.1 - Local Buffer Overflow
| windows/local/154[01;31m[K80[m[K.pl

Free Joke Script 1.0 - Authentication Bypass
| php/webapps/[01;31m[K80[m[K47.txt

FreeBSD 7.0-RELEASE - Telnet Daemon Privilege Escalation
| freebsd/local/[01;31m[K80[m[K55.txt

Freeciv Server 2.0.0beta8 - Denial of Service
| multiple/dos/8[01;31m[K80[m[K.pl

freeFTPd v1.0.13 - 'freeFTPdService' Unquoted Service Path
| windows/local/4[01;31m[K80[m[K43.txt

FreeSMS - '/pages/crc_handler.php' Multiple Cross-Site Scripting
Vulnerabilities                                |
php/webapps/38[01;31m[K80[m[K1.txt

FreeSMS - '/pages/crc_handler.php?scheduleid' SQL Injection
| php/webapps/38[01;31m[K80[m[K0.txt

freeSSHd 1.2.1 - (Authenticated) SFTP 'rename' Remote Buffer Overflow
(PoC)                                    | windows/dos/6[01;31m[K80[m[K0.pl

FreeSSHd 1.3.1 - 'FreeSSHDService' Unquoted Service Path
| windows/local/4[01;31m[K80[m[K44.txt

freeSSHd 1.3.1 - Denial of Service
| windows/dos/3[01;31m[K80[m[K01.py

freeSSHd 2.1.3 - Remote Authentication Bypass
| windows/remote/230[01;31m[K80[m[K.txt

FreeVimager 4.1.0 - Crash (PoC)
| windows/dos/232[01;31m[K80[m[K.py

fresh email script 1.0 - Multiple Vulnerabilities
| php/webapps/70[01;31m[K80[m[K.txt

FretsWeb 1.2 - 'name' Blind SQL Injection
| php/webapps/89[01;31m[K80[m[K.py

Friends in War The FAQ Manager - 'question' SQL Injection
| php/webapps/3[01;31m[K80[m[K26.txt
```

```
FTGate 7 - Cross-Site Request Forgery
| windows/webapps/383[01;31m[K80[m[K.txt

FTP Client (Ubuntu 11.04) - Local Buffer Overflow Crash (PoC)
| linux/dos/17[01;31m[K80[m[K6.txt

FTPDummy 4.[01;31m[K80[m[K - Local Buffer Overflow (SEH)
| windows/local/48685.py

FTPShell Server 6.[01;31m[K80[m[K - Buffer Overflow (SEH)
| windows/local/44713.py

FTPShell Server 6.[01;31m[K80[m[K - Denial of Service
| windows_x86/dos/44717.txt

FUDforum 3.0.6 - Cross-Site Scripting / Cross-Site Request Forgery
| php/webapps/40[01;31m[K80[m[K2.txt

FUDforum 3.0.6 - Local File Inclusion
| php/webapps/40[01;31m[K80[m[K3.txt

Furukawa Electric ConsciusMAP 2.8.1 - Remote Code Execution
| java/webapps/483[01;31m[K80[m[K.txt

FuseTalk Forum 4.0 - Multiple Cross-Site Scripting Vulnerabilities
| cfm/webapps/246[01;31m[K80[m[K.txt

FusionInvoice 2023-1.0 - Stored XSS (Cross-Site Scripting)
| multiple/webapps/514[01;31m[K80[m[K.txt

Gadu-Gadu 10.5 - Remote Code Execution
| multiple/remote/35[01;31m[K80[m[K5.txt

Gaeste 1.6 - 'gastbuch.php' Remote File Disclosure
| php/webapps/[01;31m[K80[m[K27.txt

GameHouse dldisplay - ActiveX control 0 / Real Server 5.0/7.0 Internal
IP Address Disclosure               |
windows/remote/19[01;31m[K80[m[K5.txt

Ganglia Web Frontend < 3.5.1 - PHP Code Execution
| php/webapps/3[01;31m[K80[m[K30.php

Gazelle CMS - Cross-Site Request Forgery
| php/webapps/116[01;31m[K80[m[K.txt

GDivX Zenith Player AviFixer Class - 'fix.dll 1.0.0.1' Buffer Overflow
(PoC)                               |
windows/dos/94[01;31m[K80[m[K.html

Generation Terrorists Designs & Concepts Sojourn 2.0 - File Access
| cgi/remote/19[01;31m[K80[m[K8.txt
```

GENU CMS 2012.3 - Multiple SQL Injections
| php/webapps/18[01;31m[K80[m[K9.txt

GeoVision Digital Video Surveillance System 8.2 - Arbitrary File Disclosure |
windows/remote/[01;31m[K80[m[K41.txt

GeoVision LiveX 8200 - ActiveX 'LIVEX_~1.OCX' File Corruption
| windows/remote/[01;31m[K80[m[K59.html

Gestionale Open 12.00.00 - 'DB_GO_[01;31m[K80[m[K' Unquoted Service Path |
windows/local/51065.txt

GetSimpleCMS - Unauthenticated Remote Code Execution (Metasploit)
| php/remote/468[01;31m[K80[m[K.rb

GFax 0.7.6 - Temporary Files Local Arbitrary Command Execution
| linux/local/302[01;31m[K80[m[K.txt

GFI Faxmaker Fax Viewer 10.0 (build 237) - Denial of Service (PoC)
| windows/dos/1[01;31m[K80[m[K43.py

GIMP 2.2.14 - '.ras' SUNRAS Plugin Buffer Overflow
| windows/local/3[01;31m[K80[m[K1.c

GlassFish Enterprise Server 2.1 - Admin Console '/configuration/auditModuleEdit.jsf?name' Cross-Site Scrip |
multiple/remote/329[01;31m[K80[m[K.txt

GLLCTS2 - 'sort' Blind SQL Injection
| php/webapps/5[01;31m[K80[m[K6.pl

Gnome Fonts Viewer 3.34.0 - Heap Corruption
| linux/local/48[01;31m[K80[m[K3.py

GnomeHack 1.0.5 - Local Buffer Overflow
| linux/local/1[01;31m[K80[m[K.c

GNU Mailman 2.0.x - Admin Login Cross-Site Scripting
| cgi/webapps/214[01;31m[K80[m[K.txt

GNU MyProxy 20030629 - Cross-Site Scripting
| linux/remote/23[01;31m[K80[m[K1.txt

GnuPG 1.4.3/1.9.x - Parse_User_ID Remote Buffer Overflow
| linux/dos/2[01;31m[K80[m[K77.txt

GoAutoDial CE 3.3-140608[01;31m[K80[m[K00 - Authentication Bypass / Arbitrary File Upload / Command Injection |
php/webapps/36[01;31m[K80[m[K7.txt

GOMPlayer 2.2.53.5169 - '.wav' Crash (PoC)
| windows/dos/2[01;31m[K80[m[K[01;31m[K80[m[K.py

GoodTech SSH - 'SSH_FXP_OPEN' Remote Buffer Overflow
| windows/remote/6[01;31m[K80[m[K4.pl

Google Android Broadcom Wi-Fi Driver - Memory Corruption
| android/dos/39[01;31m[K80[m[K1.c

Google Chrome - Denial of Service
| multiple/dos/1[01;31m[K80[m[K25.txt

Google Chrome - Killing Thread (PoC)
| windows/dos/1[01;31m[K80[m[K19.txt

Google Chrome 60.0.30[01;31m[K80[m[K.5 V8 JavaScript Engine - Out-of-Bounds Write |
linux/remote/42078.js

Google Chrome [01;31m[K80[m[K - JSCreate Side-effect Type Confusion (Metasploit) |
multiple/remote/48186.rb

Google Chrome [01;31m[K80[m[K.0.3987.87 - Heap-Corruption Remote Denial of Service (PoC) | windows/dos/48237.txt

Google Invisible RECAPTCHA 3 - Spoof Bypass
| multiple/webapps/4[01;31m[K80[m[K27.txt

Got All Media 7.0.0.3 - Remote Denial of Service
| windows/dos/[01;31m[K80[m[K84.pl

GOUAE DWD Realty - 'Password' SQL Injection
| asp/webapps/30[01;31m[K80[m[K7.txt

GPON Home Router FTP G-93RG1 - Cross-Site Request Forgery / Command Execution |
hardware/webapps/3[01;31m[K80[m[K73.html

Graugon Forum 1 - 'id' Command Injection / SQL Injection
| php/webapps/[01;31m[K80[m[K89.pl

Graugon Gallery 1.0 - Cross-Site Scripting / SQL Injection / Cookie Bypass |
php/webapps/[01;31m[K80[m[K40.txt

GreenBrowser 6.4.0515 - Heap Overflow
| windows/dos/2[01;31m[K80[m[K49.html

Greenstone - Multiple Vulnerabilities
| multiple/remote/3[01;31m[K80[m[K49.txt

Grestul 1.x - Cookie Authentication Bypass
| php/webapps/[01;31m[K80[m[K69.txt

GTA SA-MP - 'server.cfg' Local Buffer Overflow (Metasploit)
| windows/local/1[01;31m[K80[m[K38.rb

GTX CMS 2013 Optima - SQL Injection
| php/webapps/292[01;31m[K80[m[K.txt

GWExtranet 3.0 - 'Scp.dll' Multiple HTML Injection Vulnerabilities
| cgi/webapps/30[01;31m[K80[m[K8.txt

H&H Solutions WebSoccer 2.[01;31m[K80[m[K - 'id' SQL Injection
| php/webapps/32541.txt

Half-Life ClanMod 1.[01;31m[K80[m[K/1.81 Plugin - Remote Format String
| multiple/remote/22139.c

Hamster Audio Player 0.3a - 'Associations.cfg' Local Buffer (SEH) (2)
| windows/local/95[01;31m[K80[m[K.pl

Hanterm 3.3 - Local Buffer Overflow (1)
| linux/local/212[01;31m[K80[m[K.c

Hasura GraphQL 1.3.3 - Remote Code Execution
| multiple/webapps/49[01;31m[K80[m[K2.py

Hasura GraphQL 2.2.0 - Information Disclosure
| multiple/webapps/50[01;31m[K80[m[K3.py

HEAT Call Logging 8.01 - SQL Injection
| asp/webapps/9[01;31m[K80[m[K9.txt

Hedgehog-CMS 1.21 - Local File Inclusion / Remote Command Execution
| php/webapps/[01;31m[K80[m[K28.pl

Hedgehog-CMS 1.21 - Remote Command Execution
| php/webapps/[01;31m[K80[m[K15.pl

HeidiSQL 9.5.0.5196 - Denial of Service (PoC)
| windows/dos/45[01;31m[K80[m[K6.py

Hex Workshop v6.7 - Buffer overflow DoS
| windows/dos/510[01;31m[K80[m[K.txt

HiSilicon DVR/NVR hi3520d firmware - Remote Backdoor Account
| hardware/remote/4[01;31m[K80[m[K04.c

HomeAutomation 3.3.2 - Authentication Bypass
| php/webapps/47[01;31m[K80[m[K7.txt

HomeAutomation 3.3.2 - Cross-Site Request Forgery (Add Admin)
| php/webapps/47[01;31m[K80[m[K8.txt

HomeAutomation 3.3.2 - Persistent Cross-Site Scripting
| hardware/webapps/47[01;31m[K80[m[K6.txt

HomeAutomation 3.3.2 - Remote Code Execution
| php/webapps/47[01;31m[K80[m[K9.txt

HomeGuard Pro 9.3.1 - Insecure Folder Permissions
| windows/local/4[01;31m[K80[m[K68.txt

HooToo Tripmate HT-TM01 2.000.022 - Cross-Site Request Forgery
| hardware/webapps/3[01;31m[K80[m[K81.txt

Hot or Not Clone by Jnshosts.com - Database Backup Dump
| php/webapps/4[01;31m[K80[m[K4.txt

HotPlug CMS 1.0 - 'Login1.php' Cross-Site Scripting
| php/webapps/2[01;31m[K80[m[K31.txt

HP Data Protector Media Operations 6.20 - Directory Traversal
| windows/webapps/1[01;31m[K80[m[K77.txt

HP LoadRunner - 'magentproc.exe' Remote Overflow (Metasploit)
| windows/remote/28[01;31m[K80[m[K9.rb

HP LoadRunner - lrFileIOService ActiveX WriteFileString Remote Code
Execution (Metasploit) |
windows/remote/2[01;31m[K80[m[K83.rb

HP LoadRunner 9.5 - Remote file creation (PoC)
| windows/dos/9[01;31m[K80[m[K6.html

HP Mercury Quality Center - ActiveX Control ProgColor Buffer Overflow
(Metasploit) |
windows/remote/165[01;31m[K80[m[K.rb

HP OpenView Network Node Manager (OV NNM) - 'getnnmdata.exe' CGI
Invalid MaxAge Remote Code Execution |
windows/remote/141[01;31m[K80[m[K.py

HP OpenView Network Node Manager (OV NNM) - 'OpenView5.exe' CGI Buffer
Overflow (Metasploit) |
windows/remote/16[01;31m[K80[m[K5.rb

HP OpenView Network Node Manager (OV NNM) - 'Snmp.exe' CGI Buffer
Overflow (Metasploit) |
cgi/remote/167[01;31m[K80[m[K.rb

HP Power Manager - 'formExportDataLogs' Remote Buffer Overflow
(Metasploit) |
cgi/remote/1[01;31m[K80[m[K15.rb

HP System Event 1.2.9.0 - 'HPWMISVC' Unquoted Service Path
| windows/local/4[01;31m[K80[m[K75.txt

```
HP System Event Utility - Local Privilege Escalation
| windows/local/4[01;31m[K80[m[K57.txt

HP Tru64/OSF1 DXTerm - Local Buffer Overflow
| unix/local/21[01;31m[K80[m[K7.pl

HP Web Jetadmin 7.5.2456 - Arbitrary Command Execution
| windows/remote/238[01;31m[K80[m[K.txt

html-edit CMS - Multiple Vulnerabilities
| php/webapps/15[01;31m[K80[m[K0.txt

Huawei (Multiple Products) - Password Encryption
| hardware/remote/3[01;31m[K80[m[K20.py

Huawei DG[01;31m[K80[m[K45 Router 1.0 - Credential Disclosure
| hardware/webapps/50701.txt

Huawei SmartAX MT8[01;31m[K80[m[K - Multiple Cross-Site Request Forgery
Vulnerabilities                                  |
hardware/remote/9503.txt

Huawei UTPS - Unquoted Service Path Privilege Escalation
| windows/local/40[01;31m[K80[m[K7.txt

Hycus CMS 1.0.1 - Multiple Cross-Site Request Forgery Vulnerabilities
| php/webapps/14[01;31m[K80[m[K2.html

i-dreams GB 5.4 Final - 'admin.dat' File Disclosure
| cgi/webapps/[01;31m[K80[m[K86.txt

i-dreams GB Server - 'admin.dat' File Disclosure
| cgi/webapps/[01;31m[K80[m[K87.txt

i-dreams Mailer 1.2 Final - 'admin.dat' File Disclosure
| cgi/webapps/[01;31m[K80[m[K85.txt

I-Escorts Directory - 'country_escorts.php?country_id' SQL Injection
| php/webapps/10[01;31m[K80[m[K9.txt

I-Mall Commerce - 'i-mall.cgi' Remote Command Execution
| cgi/webapps/9[01;31m[K80[m[K.pl

I-Net MLM Script Engine - SQL Injection
| php/webapps/140[01;31m[K80[m[K.txt

I-RATER Basic - Arbitrary File Upload
| php/webapps/10[01;31m[K80[m[K0.txt

Iamma Simple Gallery 1.0/2.0 - Arbitrary File Upload
| php/webapps/6[01;31m[K80[m[K3.txt
```

IBM AIX 5.x - 'Invscout' Local Buffer Overflow
| aix/dos/25[01;31m[K80[m[K7.txt

IBM Installation Manager 1.3.0 - 'iim://' URI handler
| windows/remote/9[01;31m[K80[m[K2.html

IBM Lotus Notes 6.5.x - 'names.nsf' Cross-Site Scripting
| multiple/remote/337[01;31m[K80[m[K.txt

IBM Tivoli Storage Manager FastBack Server 5.5.4.2 -
'_FXCLI_GetConfFileChunk' Stack Buffer Overflow (PoC) |
windows/dos/389[01;31m[K80[m[K.py

IC-T-Shirt 1.2 - 'key' SQL Injection
| php/webapps/426[01;31m[K80[m[K.txt

Ice HRM 26.2.0 - Cross-Site Request Forgery (Add User)
| php/webapps/4[01;31m[K80[m[K82.txt

IceBB 1.0-rc5 - Remote Create Admin
| php/webapps/35[01;31m[K80[m[K.pl

IceWarp Universal WebMail - '/admin/inc/include.php' Multiple Remote
File Inclusions |
php/webapps/269[01;31m[K80[m[K.txt

IconCool MP3 WAV Converter 3.00 Build 120518 - Stack Buffer Overflow
| windows/dos/248[01;31m[K80[m[K.pl

ideacart 0.02 - Local File Inclusion / SQL Injection
| php/webapps/[01;31m[K80[m[K49.txt

IF-CMS 2.0 - 'id' Blind SQL Injection
| php/webapps/[01;31m[K80[m[K07.php

IF-CMS 2.07 - Local File Inclusion (1)
| php/webapps/169[01;31m[K80[m[K.py

IFOBS - 'regclientprint.jsp' Multiple HTML Injection Vulnerabilities
| jsp/webapps/37[01;31m[K80[m[K2.html

iFoto 0.20 - 'index.php' Cross-Site Scripting
| php/webapps/2[01;31m[K80[m[K11.txt

iFusion iFlance 1.1 - Multiple Input Validation Vulnerabilities
| php/webapps/2[01;31m[K80[m[K15.txt

iLife iPhoto Photocast - XML Title Remote Format String (PoC)
| osx/dos/30[01;31m[K80[m[K.rb

Image Sharing Script 4.13 - Multiple Vulnerabilities
| php/webapps/410[01;31m[K80[m[K.txt

```
ImgSvr 0.6.5 - POST Denial of Service
| windows/dos/19[01;31m[K80[m[K.pl

Incredible PBX 2.0.6.5.0 - Remote Command Execution
| php/webapps/350[01;31m[K80[m[K.pl

Indexu 5.0.1 - Multiple Remote File Inclusions
| php/webapps/2[01;31m[K80[m[K38.txt

Indexu 5.0/5.3 - 'tell_friend.php' Multiple Cross-Site Scripting
Vulnerabilities                              |
php/webapps/294[01;31m[K80[m[K.txt

Inktomi Traffic Server 4/5 - Traffic_Manager Path Argument Buffer
Overflow                                     |
linux/dos/215[01;31m[K80[m[K.txt

INNEO Startup TOOLS 2018 M040 13.0.70.3[01;31m[K80[m[K4 - Remote Code
Execution                                                |
multiple/webapps/48693.go

InselPhoto 1.1 - 'query' SQL Injection
| php/webapps/[01;31m[K80[m[K45.pl

InselPhoto 1.1 - Cross-Site Scripting
| php/webapps/[01;31m[K80[m[K57.txt

Intel 2200BG [01;31m[K80[m[K2.11 - Beacon frame Kernel Memory
Corruption                                                  |
multiple/dos/2949.c

Intel 2200BG [01;31m[K80[m[K2.11 - disassociation packet Kernel Memory
Corruption                                          | windows/dos/3224.c

Intel(R) Audio Service x64 01.00.10[01;31m[K80[m[K.0 -
'IntelAudioService' Unquoted Service Path                          |
windows/local/49929.txt

IntelliTamper 2.07 - '.map' Local Arbitrary Code Execution (1)
| windows/local/1[01;31m[K80[m[K6.c

InterSystems Cache - UtilConfigHome.csp Argument Buffer Overflow
(Metasploit)                                 |
windows/remote/16[01;31m[K80[m[K7.rb

Intuit QuickBooks Desktop 2007 < 2016 - Arbitrary Code Execution
| windows/local/39[01;31m[K80[m[K4.txt

InverseFlow 2.4 - Cross-Site Request Forgery (Add Admin)
| php/webapps/1[01;31m[K80[m[K22.txt
```

```
Invision Community Blog 1.0/1.1 - Multiple Input Validation
Vulnerabilities                                    |
php/webapps/25[01;31m[K80[m[K8.txt

Invision Gallery 2.0.5 - SQL Injection
| php/webapps/241[01;31m[K80[m[K.txt

Invision Gallery < 1.0.1 - SQL Injection
| php/webapps/43[01;31m[K80[m[K7.txt

Invision Power Board (IP.Board) < 1.3 - SQL Injection
| php/webapps/43[01;31m[K80[m[K0.txt

Invision Power Board 1.x - 'ST' SQL Injection
| php/webapps/253[01;31m[K80[m[K.txt

Invision Power Services Invision Gallery 1.0.1/1.3 - SQL Injection
| php/webapps/25[01;31m[K80[m[K6.txt

Invision Power Top Site List < 1.1 RC 2 - SQL Injection
| php/webapps/43[01;31m[K80[m[K6.txt

iOS 12.1.3 - 'cfprefsd' Memory Corruption
| ios/dos/46[01;31m[K80[m[K3.c

iOS/macOS - Out-of-Bounds Timestamp Write in
IOAccelCommandQueue2::processSegmentKernelCommand()           |
multiple/dos/4[01;31m[K80[m[K35.txt

IP2location.dll 1.0.0.1 - Function 'Initialize()' Local Buffer Overflow
| windows/local/12[01;31m[K80[m[K3.html

IP3 Networks IP3 NetAccess Appliance - SQL Injection
| hardware/remote/23[01;31m[K80[m[K8.txt

Ipswitch IMail 5.0/6.0 - Web Service Buffer Overflow (Denial of
Service) (PoC)                                     |
multiple/dos/193[01;31m[K80[m[K.txt

IrfanView - '.RLE' Image Decompression Buffer Overflow
| windows/dos/226[01;31m[K80[m[K.txt

IRIS Citations Management Tool - (Authenticated) Remote Command
Execution                                          |
php/webapps/244[01;31m[K80[m[K.txt

IRIX 5.3/6.x - 'netprint' Arbitrary Shared Library Usage
| irix/local/20[01;31m[K80[m[K4.c

ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow (3)
| solaris/remote/2[01;31m[K80[m[K.c
```

```
ISC INN 2.2 / RedHat Linux 6.0 - inews Buffer Overflow
| multiple/local/194[01;31m[K80[m[K.c

ISPConfig 2.2.3 - Multiple Remote File Inclusions
| php/webapps/2[01;31m[K80[m[K27.txt

ISPmanager 4.2.15 - Responder Privilege Escalation
| linux/local/307[01;31m[K80[m[K.txt

Jara 1.6 - Multiple Vulnerabilities
| php/webapps/1[01;31m[K80[m[K69.txt

Jara 1.6 - SQL Injection
| php/webapps/1[01;31m[K80[m[K20.txt

Jax Guestbook 3.31/3.50 - 'jax_Guestbook.php' Cross-Site Scripting
| php/webapps/315[01;31m[K80[m[K.txt

JBoss - DeploymentFileRepository WAR Deployment (via JMXInvokerServlet)
(Metasploit)                          |
multiple/remote/210[01;31m[K80[m[K.rb

jbShop e107 7 CMS Plugin - SQL Injection
| php/webapps/1[01;31m[K80[m[K56.txt

Jenkins Software RakNet 3.72 - Remote Integer Underflow
| multiple/remote/33[01;31m[K80[m[K2.txt

jetAudio 8.0.16.2000 Plus VX - '.wav' Crash (PoC)
| windows/dos/2[01;31m[K80[m[K79.py

JFrog Artifactory < 7.25.4 - Blind SQL Injection
| php/webapps/51[01;31m[K80[m[K6.py

Ji-takz - Remote File Inclusion
| php/webapps/2[01;31m[K80[m[K34.txt

jiNa OCR Image to Text 1.0 - Denial of Service (PoC)
| windows_x86/dos/453[01;31m[K80[m[K.py

JiRo's Upload System 1.0 - 'login.asp' SQL Injection
| asp/webapps/257[01;31m[K80[m[K.txt

JNM Guestbook 3.0 - 'index.php' Cross-Site Scripting
| php/webapps/34[01;31m[K80[m[K6.txt

JNM Solutions DB Top Sites 1.0 - 'vote.php' Cross-Site Scripting
| php/webapps/34[01;31m[K80[m[K7.txt

jobappr 1.4 - Multiple Vulnerabilities
| php/webapps/15[01;31m[K80[m[K4.txt
```

Joomla! / Mambo Component gigCalendar 1.0 - 'banddetails.php' SQL Injection |
php/webapps/32[01;31m[K80[m[K7.txt

Joomla! / Mambo Component Referenzen - 'id' SQL Injection
| php/webapps/312[01;31m[K80[m[K.txt

Joomla! Component Affiliate Datafeeds 8[01;31m[K80[m[K - Local File Inclusion |
php/webapps/12088.txt

Joomla! Component Alameda 1.0 - SQL Injection
| php/webapps/1[01;31m[K80[m[K58.txt

Joomla! Component Barter Sites 1.3 - Multiple Vulnerabilities
| php/webapps/1[01;31m[K80[m[K46.txt

Joomla! Component BF Quiz 1.3.0 - SQL Injection (1)
| php/webapps/127[01;31m[K80[m[K.txt

Joomla! Component com_acprojects - SQL Injection
| php/webapps/114[01;31m[K80[m[K.txt

Joomla! Component com_discussions - SQL Injection
| php/webapps/183[01;31m[K80[m[K.txt

Joomla! Component com_doc - SQL Injection
| php/webapps/50[01;31m[K80[m[K.txt

Joomla! Component com_jeemasms 3.2 - Multiple Vulnerabilities
| php/webapps/1[01;31m[K80[m[K47.txt

Joomla! Component com_jnewsletter - SQL Injection
| php/webapps/13[01;31m[K80[m[K4.txt

Joomla! Component com_jsubscription - SQL Injection
| php/webapps/13[01;31m[K80[m[K0.txt

Joomla! Component com_rsgallery2 1.14.x/2.x - Remote Backdoor Access
| php/webapps/8[01;31m[K80[m[K1.txt

Joomla! Component com_worldrates - Local File Inclusion
| php/webapps/121[01;31m[K80[m[K.txt

Joomla! Component com_xgallery 1.0 - Local File Inclusion
| php/webapps/15[01;31m[K80[m[K1.txt

Joomla! Component com_yjcontactus - Local File Inclusion
| php/webapps/1[01;31m[K80[m[K33.txt

Joomla! Component Daily Message 1.0.3 - 'id' SQL Injection
| php/webapps/6[01;31m[K80[m[K2.txt

Joomla! Component DentroVideo 1.2 - 'upload.php' Arbitrary File Upload
| php/webapps/373[01;31m[K80[m[K.php

Joomla! Component Groovy Gallery 1.0.0 - SQL Injection
| php/webapps/413[01;31m[K80[m[K.txt

Joomla! Component HM Community - Multiple Vulnerabilities
| php/webapps/1[01;31m[K80[m[K50.txt

Joomla! Component ionFiles 4.4.2 - File Disclosure
| php/webapps/6[01;31m[K80[m[K9.txt

Joomla! Component jVideoDirect - Blind SQL Injection
| php/webapps/112[01;31m[K80[m[K.txt

Joomla! Component MosReporter 0.9.3 - Remote File Inclusion
| php/webapps/2[01;31m[K80[m[K7.pl

Joomla! Component Parcoauto - 'idVeicolo' SQL Injection
| php/webapps/3[01;31m[K80[m[K08.txt

Joomla! Component ProDesk 1.0/1.2 - Local File Inclusion
| php/webapps/69[01;31m[K80[m[K.txt

Joomla! Component Restaurante 1.0 - 'id' SQL Injection
| php/webapps/52[01;31m[K80[m[K.txt

Joomla! Component Techfolio 1.0 - SQL Injection
| php/webapps/1[01;31m[K80[m[K42.txt

Joomla! Component Vik Real Estate 1.0 - Multiple Vulnerabilities
| php/webapps/1[01;31m[K80[m[K48.txt

jPORTAL 2.3.1 & UserPatch - 'forum.php' Remote Code Execution
| php/webapps/4[01;31m[K80[m[K7.php

JSPMySQL Administrador - Multiple Vulnerabilities
| jsp/webapps/3[01;31m[K80[m[K98.txt

KAPhotoservice 7.5 - 'album.asp?cat' Cross-Site Scripting
| asp/webapps/2[01;31m[K80[m[K02.txt

KAPhotoservice 7.5 - 'albums.asp?albumid' Cross-Site Scripting
| asp/webapps/2[01;31m[K80[m[K03.txt

KAPhotoservice 7.5 - 'edtalbum.asp' Multiple Cross-Site Scripting
Vulnerabilities |
asp/webapps/2[01;31m[K80[m[K04.txt

Kaspersky Internet Security 2013 - Denial of Service
| windows/dos/245[01;31m[K80[m[K.txt

KDE 1.1.2 KApplication configfile - Local Privilege Escalation (2)
| linux/local/199[01;31m[K80[m[K.pl

KDE FTP - KIOSlave URI Arbitrary FTP Server Command Execution
| linux/remote/24[01;31m[K80[m[K1.txt

Kensei Board 2.0.0b - Multiple SQL Injections
| php/webapps/8[01;31m[K80[m[K2.txt

Kentico CMS 5.5R2.23 - 'userContextMenu_Parameter' Cross-Site Scripting
| asp/webapps/35[01;31m[K80[m[K7.txt

Kerio MailServer 5.6.3 - Web Mail DO_MAP Module Cross-Site Scripting
| cgi/webapps/22[01;31m[K80[m[K4.txt

Kerio MailServer 5.6.3 add_acl Module - Overflow
| linux/dos/22[01;31m[K80[m[K1.txt

Kerio MailServer 5.6.3 do_map Module - Overflow
| linux/dos/22[01;31m[K80[m[K3.txt

Kerio MailServer 5.6.3 list Module - Overflow
| linux/dos/22[01;31m[K80[m[K2.txt

Kerio MailServer 5.6.3 subscribe Module - Overflow
| linux/dos/22[01;31m[K80[m[K0.txt

Kerio Personal Firewall 2.1.x/4.x - Local Denial of Service
| multiple/dos/24[01;31m[K80[m[K9.txt

Kimai 1.14 - CSV Injection
| php/webapps/49[01;31m[K80[m[K5.txt

KingView 6.53 - 'KChartXY' ActiveX File Creation / Overwrite
| windows/local/2[01;31m[K80[m[K85.html

KingView 6.53 - 'SuperGrid' Insecure ActiveX Control
| windows/local/2[01;31m[K80[m[K84.html

Kirby CMS 3.5.3.1 - 'file' Cross-Site Scripting (XSS)
| php/webapps/49[01;31m[K80[m[K8.txt

Kiwi CatTools TFTP 3.2.8 - Directory Traversal
| windows/remote/33[01;31m[K80[m[K.txt

kloxo 5.75 - Multiple Vulnerabilities
| linux/remote/88[01;31m[K80[m[K.txt

KMPlayer 2.9.3.1214 - Multiple Remote Denial of Service Vulnerabilities
| linux/dos/305[01;31m[K80[m[K.txt

KnFTP 1.0 - Remote Buffer Overflow (DEP Bypass) (Metasploit)
| windows/remote/1[01;31m[K80[m[K89.rb

```
kontakt formular 1.1 - Remote File Inclusion
| php/webapps/14[01;31m[K80[m[K9.txt

Kordil EDms 2.2.60rc3 - SQL Injection
| php/webapps/231[01;31m[K80[m[K.txt

Kronos WebTA 4.0 - Authenticated Remote Privilege Escalation
| java/webapps/4[01;31m[K80[m[K01.py

Ktools Photostore 3.5.1 - 'gid' SQL Injection
| php/webapps/55[01;31m[K80[m[K.txt

KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 - Command Injection
(Authenticated)                          |
hardware/webapps/496[01;31m[K80[m[K.txt

LabStoRe 1.5.4 - SQL Injection
| php/webapps/1[01;31m[K80[m[K90.txt

LabVantage 8.3 - Information Disclosure
| java/webapps/4[01;31m[K80[m[K90.py

Land Down Under 601/602/700/701/[01;31m[K80[m[K0/[01;31m[K80[m[K1 -
'events.php' HTML Injection                                          |
php/webapps/26223.txt

Land Down Under 700/701/[01;31m[K80[m[K0/[01;31m[K80[m[K1 -
'events.php?c' SQL Injection
| php/webapps/26206.txt

Land Down Under 700/701/[01;31m[K80[m[K0/[01;31m[K80[m[K1 -
'index.php?c' SQL Injection
| php/webapps/26205.txt

Land Down Under 700/701/[01;31m[K80[m[K0/[01;31m[K80[m[K1 - 'list.php'
Multiple SQL Injections                                              |
php/webapps/26207.txt

Land Down Under [01;31m[K80[m[K0 - 'index.php' Multiple Cross-Site
Scripting Vulnerabilities                                |
php/webapps/26182.txt

Land Down Under [01;31m[K80[m[K0 - 'journal.php?w' Cross-Site Scripting
| php/webapps/26181.txt

Land Down Under [01;31m[K80[m[K0/[01;31m[K80[m[K1 - 'auth.php?m' SQL
Injection                                                            |
php/webapps/26253.txt

Land Down Under [01;31m[K80[m[K0/[01;31m[K80[m[K1 - 'forums.php'
Multiple SQL Injections                                                |
php/webapps/261[01;31m[K80[m[K.txt
```

```
Land Down Under [01;31m[K80[m[K0/[01;31m[K80[m[K1 - 'journal.php?m' SQL
Injection                                                    |
php/webapps/26178.txt

Land Down Under [01;31m[K80[m[K0/[01;31m[K80[m[K1 - 'links.php?w' SQL
Injection                                                     |
php/webapps/26177.txt

Land Down Under [01;31m[K80[m[K0/[01;31m[K80[m[K1 - 'list.php' Multiple
SQL Injections                                               |
php/webapps/26179.txt

Land Down Under [01;31m[K80[m[K0/[01;31m[K80[m[K1 - 'plug.php?e' SQL
Injection                                                     |
php/webapps/26254.txt

LANDesk Management Suite 8.[01;31m[K80[m[K.1.1 - PXE TFTP Service
Directory Traversal                                  |
linux/remote/31591.txt

Lanifex DMO 2.3b - '_incMgr' Remote File Inclusion
| php/webapps/22[01;31m[K80[m[K.pl

lastRSS autoposting bot MOD 0.1.3 - 'phpbb_root_path' Remote File
Inclusion                                  |
php/webapps/32[01;31m[K80[m[K4.txt

LeadTools Imaging LEADSmtp - ActiveX Control 'SaveMessage()' Insecure
Method                                |
windows/remote/358[01;31m[K80[m[K.html

LearnLoop 2.0beta7 - 'sFilePath' Remote File Disclosure
| php/webapps/46[01;31m[K80[m[K.txt

Lenovo RapidBoot HDD Accelerator 1.00.0[01;31m[K80[m[K2 - Unquoted
Service Path Privilege Escalation                    |
windows/local/405[01;31m[K80[m[K.txt

LEPTON 2.2.2 - Remote Code Execution
| php/webapps/40[01;31m[K80[m[K1.txt

LEPTON 2.2.2 - SQL Injection
| php/webapps/40[01;31m[K80[m[K0.txt

Level One Enterprise Access Point (Multiple Devices) - 'backupCfg.cgi'
Security Bypass                      |
hardware/remote/38[01;31m[K80[m[K4.py

Lexmark Multiple Laser printers - Remote Stack Overflow
| hardware/dos/118[01;31m[K80[m[K.txt

libextractor 0.5.13 - Multiple Heap Overflows (PoC)
| multiple/dos/1[01;31m[K80[m[K1.txt
```

```
LibreHealth 2.0.0 - (Authenticated) Arbitrary File Actions
| php/webapps/45[01;31m[K80[m[K2.txt

LibSPF2 < 1.2.8 - DNS TXT Record Parsing Bug Heap Overflow (PoC)
| multiple/dos/6[01;31m[K80[m[K5.txt

Liferay CE < 6.2 CE GA6 - Persistent Cross-Site Scripting
| jsp/webapps/398[01;31m[K80[m[K.txt

Linksys BEFVP4 - SNMP Community String Information Disclosure
| hardware/remote/224[01;31m[K80[m[K.txt

Linksys WAP11 1.3/1.4 / D-Link DI-[01;31m[K80[m[K4 4.68/Dl-704 2.56 b5
- Embedded HTTP Server Denial of Service         |
hardware/dos/21978.txt

Linux Kernel 2.6.37-rc1 - 'serial_multiport_struct' Local Information
Leak                                  |
linux/local/1[01;31m[K80[m[K[01;31m[K80[m[K.c

Linux Kernel 2.6.x - 'AIO_Free_Ring' Local Denial of Service
| linux/dos/24[01;31m[K80[m[K4.c

Linux Kernel 2.6.x - 'sock.c' SO_BSDCOMPAT Option Information
Disclosure                                      |
linux/local/32[01;31m[K80[m[K5.c

Linux Kernel 2.6.x - VFat Compat IOCTLS Local Denial of Service
| linux/dos/300[01;31m[K80[m[K.c

Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)
| linux/local/50[01;31m[K80[m[K8.c

Linux Kernel < 2.6.16.18 - Netfilter NAT SNMP Module Remote Denial of
Service                               | linux/dos/18[01;31m[K80[m[K.c

Linux Kernel < 2.6.30.5 - 'cfg[01;31m[K80[m[K211' Remote Denial of
Service                                                 | linux/dos/9442.c

LiveZilla 3.1.8.3 - Cross-Site Scripting
| php/webapps/10[01;31m[K80[m[K6.txt

Loki Download Manager 2.0 - 'Catinfo.asp' SQL Injection
| asp/webapps/25[01;31m[K80[m[K5.txt

Loki Download Manager 2.0 - 'default.asp' SQL Injection
| asp/webapps/25[01;31m[K80[m[K4.txt

Lotus Domino 8.5.3 - 'EXAMINE' Stack Buffer Overflow DEP/ASLR Bypass
(NSA's EMPHASISMINE)                   |
windows/remote/46[01;31m[K80[m[K8.py
```

```
LoudBlog 0.8.0a - 'ajax.php' SQL Injection
| php/webapps/6[01;31m[K80[m[K8.pl

Lycos HTMLGear - guestGear CSS HTML Injection
| cgi/webapps/21[01;31m[K80[m[K2.txt

M/Monit 3.7.4 - Privilege Escalation
| multiple/webapps/490[01;31m[K80[m[K.py

MA Lighting Technology grandMA onPC 6.[01;31m[K80[m[K8 - Remote Denial
of Service                                        | windows/dos/32704.pl

MachForm < 4.2.3 - SQL Injection / Path Traversal / Upload Bypass
| php/webapps/44[01;31m[K80[m[K4.txt

macOS 10.13 (17A365) - Kernel Memory Disclosure due to Lack of Bounds
Checking in 'AppleIntelCapriControll | macos/dos/437[01;31m[K80[m[K.c

Macrovision SafeDisc - 'SecDRV.SYS' Method_Neither Privilege Escalation
| windows/local/306[01;31m[K80[m[K.txt

Magento 1.2 -
'/app/code/core/Mage/Admin/Model/Session.php?login['Username']' Cross-
Site Scripting         | php/webapps/32[01;31m[K80[m[K8.txt

Magento 1.2 -
'/app/code/core/Mage/Adminhtml/controllers/IndexController.php?email'
Cross-Site Scripting   | php/webapps/32[01;31m[K80[m[K9.txt

MailEnable - IMAPD W3C Logging Buffer Overflow (Metasploit)
| windows/remote/164[01;31m[K80[m[K.rb

Mailist 3.0 - Insecure Backup / Local File Inclusion
| php/webapps/[01;31m[K80[m[K01.txt

Mailtraq 2.1.0.1302 - Remote Format String SMTP Resource Consumption
| windows/dos/227[01;31m[K80[m[K.txt

Malwarebytes 4.5 - Unquoted Service Path
| windows/local/50[01;31m[K80[m[K6.txt

Mambo 4.6.4 - 'Output.php' Remote File Inclusion
| php/webapps/5[01;31m[K80[m[K8.txt

Mambo < 4.5 - Multiple Vulnerabilities
| php/webapps/43[01;31m[K80[m[K4.txt

Mambo Component N-Gallery - Multiple SQL Injections
| php/webapps/59[01;31m[K80[m[K.txt

ManageEngine Applications Manager Build 12700 - Multiple
Vulnerabilities                                   |
jsp/webapps/397[01;31m[K80[m[K.txt
```

```
ManageEngine Desktop Central 8.0.0 build < [01;31m[K80[m[K293 -
Arbitrary File Upload                                    |
jsp/webapps/29674.txt

ManageEngine Desktop Central 9 Build 90087 - Cross-Site Request Forgery
| multiple/webapps/359[01;31m[K80[m[K.html

ManageEngine ServiceDesk Plus 8.0 Build [01;31m[K80[m[K13 - Multiple
Cross-Site Scripting Vulnerabilities              |
jsp/webapps/17586.txt

ManageEngine ServiceDesk Plus 8.0.0 Build [01;31m[K80[m[K13 - Improper
User Privileges                                  |
multiple/webapps/17572.txt

ManageEngine Support Center Plus 7.8 Build 7[01;31m[K80[m[K1 -
Directory Traversal                                       |
jsp/webapps/17442.txt

Mantis Bug Tracker 1.2.19 - Host Header
| php/webapps/3[01;31m[K80[m[K68.txt

ManTrap 1.6.1 - Hidden Process Disclosure
| unix/local/203[01;31m[K80[m[K.c

Mara CMS 7.5 - Remote Code Execution (Authenticated)
| php/webapps/487[01;31m[K80[m[K.txt

MATLAB R2009b - 'dtoa' Implementation Memory Corruption
| linux/dos/334[01;31m[K80[m[K.txt

Maximus SchoolMAX 4.0.1 - 'Error_msg' Cross-Site Scripting
| asp/webapps/2[01;31m[K80[m[K86.txt

McAfee ePO 4.6.6 - Multiple Vulnerabilities
| windows/webapps/26[01;31m[K80[m[K7.txt

McAfee Virtual Technician 6.3.0.1911 MVT.MVTControl.6300 - ActiveX
'GetObject()' Code Execution           |
windows/remote/18[01;31m[K80[m[K5.txt

McGallery 1.0/1.1/2.2 - 'index.php?language' Traversal Local File
Inclusion                                 |
php/webapps/26[01;31m[K80[m[K8.txt

McGallery 1.0/1.1/2.2 - 'show.php' Multiple SQL Injections
| php/webapps/26[01;31m[K80[m[K9.txt

mcGuestbook 1.3 - 'admin.php?lang' Remote File Inclusion
| php/webapps/2[01;31m[K80[m[K35.txt

mcGuestbook 1.3 - 'ecrire.php?lang' Remote File Inclusion
| php/webapps/2[01;31m[K80[m[K36.txt
```

mcGuestbook 1.3 - 'lire.php?lang' Remote File Inclusion
| php/webapps/2[01;31m[K80[m[K37.txt

MD5 - Message Digest Algorithm Hash Collision
| multiple/dos/24[01;31m[K80[m[K7.txt

Media Player Classic (MPC) 1.5 - WebServer Request Handling Remote Denial of Service |
multiple/dos/3[01;31m[K80[m[K21.pl

Mediacoder 0.8.33 build 56[01;31m[K80[m[K - '.lst' Buffer Overflow (PoC) (SEH Overwrite) |
windows/dos/35531.py

Mediacoder 0.8.33 build 56[01;31m[K80[m[K - '.m3u' Buffer Overflow (PoC) (SEH Overwrite) |
windows/dos/35530.py

MediaSuite CMS - Artibary File Disclosure
| php/webapps/36[01;31m[K80[m[K4.pl

Meinberg NTP Time Server ELX[01;31m[K80[m[K0/GPS M4x V5.30p - Remote Command Execution / Escalate Privileges |
hardware/remote/40120.py

Membership Formula - 'order' SQL Injection
| php/webapps/417[01;31m[K80[m[K.txt

MemHT Portal 4.0.1 - Delete All Private Messages
| php/webapps/[01;31m[K80[m[K64.pl

Mephisto Blog 0.7.3 - Search Function Cross-Site Scripting
| php/webapps/297[01;31m[K80[m[K.txt

Merak Mail Server 7.4.5 - HTML Message Body Cross-Site Scripting
| php/webapps/243[01;31m[K80[m[K.txt

Mercury Audio Player 1.21 - '.b4s' Local Stack Overflow
| windows/local/85[01;31m[K80[m[K.py

Mercury MR[01;31m[K80[m[K4 Router - Multiple HTTP Header Fields Denial of Service Vulnerabilities |
hardware/dos/36868.pl

MetaProducts MetaTreeX 1.5.100 - ActiveX File Overwrite
| windows/remote/7[01;31m[K80[m[K4.html

Metasploit Web UI 4.1.0 - Persistent Cross-Site Scripting
| multiple/webapps/1[01;31m[K80[m[K12.txt

Michael Sandrof IrcII 4.4-7 - Remote Buffer Overflow
| linux/remote/19[01;31m[K80[m[K1.c

Micro Focus (HPE) Data Protector - SUID Privilege Escalation (Metasploit) | linux/local/475[01;31m[K80[m[K.rb

Microsoft 'Shlwapi.dll' 6.0.2[01;31m[K80[m[K0.1106 - Malformed HTML Form Tag Denial of Service | windows/dos/22518.html

Microsoft - NTLM Hash Disclosure Spoofing (library-ms) | windows/local/522[01;31m[K80[m[K.txt

Microsoft DirectX SDK - 'Xact.exe' Remote Code Execution | windows/remote/451[01;31m[K80[m[K.txt

Microsoft Edge - CBaseScriptable::PrivateQueryInterface Memory Corruption (MS16-068) | windows/dos/408[01;31m[K80[m[K.txt

Microsoft Edge Chakra JIT - 'BailOutOnTaggedValue' Bailouts Type Confusion | windows/dos/431[01;31m[K80[m[K.js

Microsoft Edge Chakra JIT - 'NewScObjectNoCtor' Array Type Confusion | windows/dos/440[01;31m[K80[m[K.js

Microsoft Excel - Denial of Service | windows/dos/379[01;31m[K80[m[K.pl

Microsoft Excel 2003 11.8335.8333 - Use-After-Free | windows/dos/1[01;31m[K80[m[K78.txt

Microsoft Excel 2007 - '.xlb' Local Buffer Overflow (MS11-021) (Metasploit) | windows/local/1[01;31m[K80[m[K87.rb

Microsoft Excel 2007 SP2 - Buffer Overwrite (MS11-021) | windows/local/1[01;31m[K80[m[K67.txt

Microsoft Exchange Server 2000/2003 - Outlook Web Access Script Injection | windows/remote/2[01;31m[K80[m[K05.pl

Microsoft IIS 2.0/3.0 - Long URL Denial of Service | windows/dos/20[01;31m[K80[m[K2.c

Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2) | windows/remote/8[01;31m[K80[m[K6.pl

Microsoft IIS 7.5 (Windows 7) - FTPSVC Unauthorized Remote Denial of Service (PoC) | windows/dos/15[01;31m[K80[m[K3.py

```
Microsoft Internet Explorer - CDisplayPointer Use-After-Free (MS13-
0[01;31m[K80[m[K) (Metasploit)                          |
windows/remote/28974.rb

Microsoft Internet Explorer - CFlatMarkupPointer Use-After-Free (MS13-
059) (Metasploit)                     |
windows/remote/2[01;31m[K80[m[K82.rb

Microsoft Internet Explorer - NCTAudioFile2.AudioFile ActiveX Remote
Stack Overflow (2)                     |
windows/remote/3[01;31m[K80[m[K8.html

Microsoft Internet Explorer 11.0.9600.1[01;31m[K80[m[K97 -
COmWindowProxy::SwitchMarkup NULL PTR                          |
windows/dos/38916.html

Microsoft Internet Explorer 5.0.1 - FTP URI Arbitrary FTP Server
Command Execution                          |
windows/remote/24[01;31m[K80[m[K0.txt

Microsoft Internet Explorer 5.0.1/5.5/6.0 - Telnet Client File
Overwrite                                    |
windows/remote/206[01;31m[K80[m[K.html

Microsoft Internet Explorer 6 - Search Pane URI Obfuscation
| windows/remote/24[01;31m[K80[m[K8.txt

Microsoft Internet Explorer 6 - Sysimage Protocol Handler Local File
Detection                                |
windows/remote/24[01;31m[K80[m[K2.txt

Microsoft Internet Explorer 6 - URI Handler Restriction Circumvention
| windows/remote/21[01;31m[K80[m[K3.txt

Microsoft Internet Explorer 6.0/7.0 - 'RemoveChild' Denial of Service
| windows/dos/288[01;31m[K80[m[K.txt

Microsoft Internet Explorer 7 (Windows 2003 SP2) - Memory Corruption
(MS09-002)                               |
windows/remote/[01;31m[K80[m[K82.html

Microsoft Internet Explorer 7 (Windows XP SP2) - Memory Corruption
(MS09-002)                                 |
windows/remote/[01;31m[K80[m[K79.html

Microsoft Internet Explorer 7 - HTML Denial of Service
| windows/dos/29[01;31m[K80[m[K0.py

Microsoft Internet Explorer 7 - Memory Corruption (MS09-002)
| windows/remote/[01;31m[K80[m[K[01;31m[K80[m[K.py

Microsoft Internet Explorer 7 - Memory Corruption (PoC) (MS09-002)
| windows/dos/[01;31m[K80[m[K77.html
```

Microsoft Internet Explorer 8/9/10/11 / IIS / CScript.exe/WScript.exe VBScript - CRegExp..Execute Use of U | windows/remote/40721.html

Microsoft Internet Explorer Windows 10 1[01;31m[K80[m[K9 17763.316 - Scripting Engine Memory Corruption | windows/remote/46928.html

Microsoft Java Virtual Machine 3[01;31m[K80[m[K2 Series - Bytecode Verifier | windows/remote/22027.txt

Microsoft Office 2003 - Embedded Shockwave Flash Object Security Bypass | windows/dos/2[01;31m[K80[m[K87.txt

Microsoft Office 2007 - 'msxml5.dll' Crash (PoC) | windows/dos/3[01;31m[K80[m[K31.pl

Microsoft Office 2007 - 'OGL.dll' DpOutputSpanStretch::OutputSpan Out of Bounds Write (MS15-0[01;31m[K80[m[K) | windows/dos/37911.txt

Microsoft Office 2019 MSO Build 1[01;31m[K80[m[K8 - NTLMv2 Hash Disclosure | windows/remote/52113.NA

Microsoft Outlook2000/Express 6.0 - Arbitrary Program Execution | windows/remote/222[01;31m[K80[m[K.txt

Microsoft People 10.1[01;31m[K80[m[K7.2131.0 - Denial of service (PoC) | windows_x86-64/dos/45335.txt

Microsoft SharePoint - Deserialization Remote Code Execution | windows/remote/4[01;31m[K80[m[K53.py

Microsoft SMB Driver - Local Denial of Service | windows/dos/2[01;31m[K80[m[K01.c

Microsoft UPnP - Local Privilege Elevation (Metasploit) | windows/local/47[01;31m[K80[m[K5.rb

Microsoft Visio 2007 - 'mfc[01;31m[K80[m[Kesn.dll' DLL Loading Arbitrary Code Execution | windows/remote/34832.c

Microsoft Visual Basic - '.VBP' Local Buffer Overflow (Metasploit) | windows/local/166[01;31m[K80[m[K.rb

Microsoft VM 2000/3000/3100/3188/3200/3300/3[01;31m[K80[m[K2/3[01;31m[K80[m[K5 series - JDBC Class Code Execution | windows/remote/21[01;31m[K80[m[K8.txt

```
Microsoft Win32k - Null Pointer De-reference (PoC) (MS11-077)
| windows/dos/1[01;31m[K80[m[K24.txt

Microsoft Windows - '.ani' GDI Remote Privilege Escalation (MS07-017)
| windows/remote/3[01;31m[K80[m[K4.txt

Microsoft Windows - 'AfdJoinLeaf' Local Privilege Escalation (MS11-
0[01;31m[K80[m[K) (Metasploit)                          |
windows/local/21844.rb

Microsoft Windows - 'NetpManageIPCConnect' Remote Stack Overflow (MS06-
070)                                    |
windows/remote/2[01;31m[K80[m[K9.py

Microsoft Windows - 'srv2.sys' SMB Code Execution (Python) (MS09-050)
| windows/remote/402[01;31m[K80[m[K.py

Microsoft Windows - 'WizardOpium' Local Privilege Escalation
| windows/local/481[01;31m[K80[m[K.cpp

Microsoft Windows - Advanced Local Procedure Call (ALPC) Local
Privilege Escalation                          |
windows/local/452[01;31m[K80[m[K.txt

Microsoft Windows - JPEG GDI+ Remote Heap Overflow (MS04-028)
| windows/remote/4[01;31m[K80[m[K.c

Microsoft Windows - MSCOMCTL ActiveX Buffer Overflow (MS12-027)
(Metasploit)                                    |
windows/remote/187[01;31m[K80[m[K.rb

Microsoft Windows - NtCreateLowBoxToken Handle Capture Local Denial of
Service / Privilege Escalation (MS1 |
windows/dos/385[01;31m[K80[m[K.txt

Microsoft Windows - Shell COM Server Registrar Local Privilege
Escalation                                      |
windows/local/478[01;31m[K80[m[K.cc

Microsoft Windows - Wkssvc NetrJoinDomain2 Stack Overflow (MS06-070)
| windows/remote/2[01;31m[K80[m[K0.cpp

Microsoft Windows 10 (Build 17134) - Local Privilege Escalation (UAC
Bypass)                                    |
windows/local/45[01;31m[K80[m[K5.cpp

Microsoft Windows 10 - Desktop Bridge Virtual Registry CVE-2018-
08[01;31m[K80[m[K Incomplete Fix Privilege Escalation   |
windows/dos/44915.txt

Microsoft Windows 10 1[01;31m[K80[m[K9 -
'CmKeyBodyRemapToVirtualForEnum' Arbitrary Key Enumeration Privilege
Escalatio | windows/local/46912.txt
```

Microsoft Windows 10 1[01;31m[K80[m[K9 - LUAFV Delayed Virtualization Cache Manager Poisoning Privilege Escalation | windows/local/46717.txt

Microsoft Windows 10 1[01;31m[K80[m[K9 - LUAFV Delayed Virtualization Cross Process Handle Duplication Privilege Escala | windows/local/46714.txt

Microsoft Windows 10 1[01;31m[K80[m[K9 - LUAFV Delayed Virtualization MAXIMUM_ACCESS DesiredAccess Privilege Escalation | windows/local/46713.txt

Microsoft Windows 10 1[01;31m[K80[m[K9 - LUAFV LuafvCopyShortName Arbitrary Short Name Privilege Escalation | windows/local/46715.txt

Microsoft Windows 10 1[01;31m[K80[m[K9 - LUAFV NtSetCachedSigningLevel Device Guard Bypass | windows/local/46716.txt

Microsoft Windows 10 1[01;31m[K80[m[K9 - LUAFV PostLuafvPostReadWrite SECTION_OBJECT_POINTERS Race Condition Privilege | windows/local/46718.txt

Microsoft Windows 10 1[01;31m[K80[m[K9 / 1709 - CSRSS SxSSrv Cached Manifest Privilege Escalation | windows/local/46712.txt

Microsoft Windows 10 1903/1[01;31m[K80[m[K9 - RPCSS Activation Kernel Security Callback Privilege Escalation | windows/local/47135.txt

Microsoft Windows 10 Build 1[01;31m[K80[m[K3 < 1903 - 'COMahawk' Local Privilege Escalation | windows/local/47684.md

Microsoft Windows 10 build 1[01;31m[K80[m[K9 - Local Privilege Escalation (UAC Bypass) | windows/local/47915.py

Microsoft Windows 7 < 10 / 2008 < 2012 (x86/x64) - Local Privilege Escalation (MS16-032) | windows/local/39[01;31m[K80[m[K9.cs

Microsoft Windows Defender - VBScript Detection Bypass | windows_x86-64/local/51[01;31m[K80[m[K2.txt

Microsoft Windows Defender Bypass - Detection Mitigation Bypass | windows_x86-64/local/51[01;31m[K80[m[K1.txt

Microsoft Windows Help Centre Handles - Malformed Escape Sequences Incorrectly (MS03-044) | windows/remote/13[01;31m[K80[m[K8.txt

Microsoft Windows HTA (HTML Application) - Remote Code Execution (MS14-064) | windows/remote/37[01;31m[K80[m[K0.php

Microsoft Windows Internet Communication Settings - 'schannel.dll' DLL Hijacking | windows/local/147[01;31m[K80[m[K.c

Microsoft Windows Kernel (7 x86) - Local Privilege Escalation (MS16-039) | windows_x86/local/444[01;31m[K80[m[K.cpp

Microsoft Windows Kernel - 'NtGdiStretchBlt' Pool Buffer Overflow (MS15-097) | windows_x86/dos/382[01;31m[K80[m[K.txt

Microsoft Windows Kernel - 'NtQueryVirtualMemory(MemoryMappedFilenameInformation)' Double-Write Ring-0 Add | windows/dos/433[01;31m[K80[m[K.cpp

Microsoft Windows Kernel - 'win32kfull!SfnINLPUAHDRAWMENUITEM' Stack Memory Disclosure | windows/dos/418[01;31m[K80[m[K.cpp

Microsoft Windows Kernel - Information Disclosure | windows/local/4[01;31m[K80[m[K71.md

Microsoft Windows Live Messenger 14 - 'dwmapi.dll' DLL Loading Arbitrary Code Execution | windows/remote/35[01;31m[K80[m[K9.c

Microsoft Windows Media Center - '.MCL' File Processing Remote Code Execution (MS16-059) | windows/remote/39[01;31m[K80[m[K5.txt

Microsoft Windows Plug-and-Play Service (French) - Remote Universal (MS05-039) | windows/remote/11[01;31m[K80[m[K.c

Microsoft Windows Server 2000 - Debug Registers | windows/local/208[01;31m[K80[m[K.c

Microsoft Windows XP/2003 - 'afd.sys' Local Privilege Escalation (MS11-0[01;31m[K80[m[K) | windows/local/18176.py

Microsoft WMITools - ActiveX Remote Command Execution | windows/remote/15[01;31m[K80[m[K9.html

Microsys PROMOTIC 8.1.4 - ActiveX GetPromoticSite Unitialized Pointer
| windows/dos/1[01;31m[K80[m[K49.txt

Mihalism Multi Forum Host 3.0.x - Remote File Inclusion
| php/webapps/4[01;31m[K80[m[K8.txt

Mihalism Multi Host - 'users.php' Cross-Site Scripting
| php/webapps/376[01;31m[K80[m[K.txt

MikroTik RouterOS - sshd (ROSSSH) Remote Heap Corruption
| hardware/remote/2[01;31m[K80[m[K56.txt

Mini-CMS / News Script Light 1.0 - Remote File Inclusion
| php/webapps/14[01;31m[K80[m[K8.pl

Mini-stream Ripper 3.0.1.1 - Local Buffer Overflow (Metasploit) (3)
| windows/local/1[01;31m[K80[m[K82.rb

miniblog 1.0.1 - Cross-Site Request Forgery (Add New Post)
| php/webapps/404[01;31m[K80[m[K.txt

MiniFtp - 'parseconf_load_setting' Buffer Overflow
| linux/local/46[01;31m[K80[m[K7.txt

minimal Gallery - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities |
php/webapps/37[01;31m[K80[m[K4.txt

MiniWebsvr 0.0.10 - Directory Traversal / Listing
| windows/remote/125[01;31m[K80[m[K.txt

MISP 2.4.171 - Stored XSS
| php/webapps/517[01;31m[K80[m[K.txt

Mitel AWC - Command Execution
| cgi/webapps/15[01;31m[K80[m[K7.txt

MKPortal NoBoard Module (Beta) - Remote File Inclusion
| php/webapps/41[01;31m[K80[m[K.txt

MLdonkey 2.9.7 - Arbitrary File Disclosure
| multiple/remote/[01;31m[K80[m[K97.txt

MoinMoin 1.x - 'PageEditor.py' Cross-Site Scripting
| cgi/webapps/340[01;31m[K80[m[K.txt

Monit 4.2 - Basic Authentication Remote Code Execution
| linux/remote/5[01;31m[K80[m[K.c

Monitorr 1.7.6m - Remote Code Execution (Unauthenticated)
| php/webapps/489[01;31m[K80[m[K.py

Monkey HTTP Server 0.1/0.4/0.5 - Multiple Cross-Site Scripting Vulnerabilities | multiple/remote/218[01;31m[K80[m[K.txt

Montiorr 1.7.6m - Persistent Cross-Site Scripting | php/webapps/49[01;31m[K80[m[K6.txt

Moodle 3.9 - Remote Code Execution (RCE) (Authenticated) | php/webapps/501[01;31m[K80[m[K.py

Motorola SBG65[01;31m[K80[m[K Cable Modem & Wireless Router - Reboot (Denial of Service) | hardware/dos/30688.py

Mozilla Firefox - Proxy Prototype Privileged JavaScript Injection (Metasploit) | multiple/remote/364[01;31m[K80[m[K.rb

Mozilla Firefox 1.0.x - JavaScript Handler Race Condition Memory Corruption | linux/dos/283[01;31m[K80[m[K.txt

Mozilla Firefox 1.5 (OSX) - 'location.QueryInterface()' Code Execution (Metasploit) | osx/remote/14[01;31m[K80[m[K.pm

Mozilla Firefox 1.5.0.3 - 'Loop' Denial of Service | multiple/dos/1[01;31m[K80[m[K2.html

Mozilla Firefox 3.0.6 - BODY onload Remote Crash | multiple/dos/[01;31m[K80[m[K91.html

Mozilla Firefox 3.6 - 'gfxTextRun::SanitizeGlyphRuns()' Remote Memory Corruption | multiple/dos/33[01;31m[K80[m[K0.html

Mozilla Firefox/Thunderbird/SeaMonkey - Multiple Memory Corruption Vulnerabilities | linux/dos/33[01;31m[K80[m[K1.txt

MP3 Wav Editor 3.[01;31m[K80[m[K - '.mp3' Local Denial of Service | windows/dos/12073.pl

MPCS 0.2 - 'comment.php' Cross-Site Scripting | php/webapps/2[01;31m[K80[m[K32.txt

Mpxplay MultiMedia Commander 2.00a - '.m3u' Stack Buffer Overflow (PoC) | windows/dos/3[01;31m[K80[m[K53.txt

MS SQL Server 2000/2005 - SQLNS.SQLNamespace COM Object Refresh() Unhandled Pointer | windows/remote/3[01;31m[K80[m[K05.asp

MSI Packages Symbolic Links Processing - Windows 10 Privilege Escalation |
windows/local/4[01;31m[K80[m[K79.txt

MSN Messenger (Linux) - '.png' Image Buffer Overflow
| windows/remote/[01;31m[K80[m[K4.c

MSN Messenger - '.png' Image Buffer Overflow Download Shellcode
| windows/remote/[01;31m[K80[m[K2.cpp

Multi Outlets POS 3.1 - 'id' SQL Injection
| php/webapps/412[01;31m[K80[m[K.txt

multi-lingual E-Commerce system 0.2 - Multiple Vulnerabilities
| php/webapps/84[01;31m[K80[m[K.txt

MultiCart 1.0 - Blind SQL Injection
| php/webapps/44[01;31m[K80[m[K.pl

Multiple PDF Readers - JBIG2 Local Buffer Overflow (PoC)
| windows/dos/[01;31m[K80[m[K90.txt

Muziic Player 2.0 - '.mp3' Local Denial of Service
| windows/dos/111[01;31m[K80[m[K.pl

MyBB OUGC Awards Plugin 1.8.3 - Persistent Cross-Site Scripting
| php/webapps/460[01;31m[K80[m[K.txt

MyBloggie 2.1.2/2.1.3 - 'upload.php' Cross-Site Scripting
| php/webapps/273[01;31m[K80[m[K.txt

MyBulletinBoard (MyBB) 1.0.x/1.1.x - 'usercp.php' SQL Injection
| php/webapps/2[01;31m[K80[m[K92.txt

MyBulletinBoard (MyBB) 1.2.5 - 'calendar.php' Blind SQL Injection
| php/webapps/37[01;31m[K80[m[K.pl

MyDNS 1.1.0 - Remote Heap Overflow (PoC)
| linux/dos/3[01;31m[K80[m[K7.c

MyForum 1.3 - Authentication Bypass
| php/webapps/8[01;31m[K80[m[K3.txt

Mynews 0.10 - Authentication Bypass
| php/webapps/[01;31m[K80[m[K34.txt

MyNews 1.6.2 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/27[01;31m[K80[m[K9.txt

MyPHP Forum 1.0 - SQL Injection
| php/webapps/[01;31m[K80[m[K7.txt

```
MySQL MaxDB 7.5 - WAHTTP Server Remote Denial of Service
| multiple/dos/24[01;31m[K80[m[K5.txt

MySQL Server 4/5 - Str_To_Date Remote Denial of Service
| linux/dos/2[01;31m[K80[m[K26.txt

MyVideoConverter Pro 3.14 - 'Movie' Buffer Overflow
| windows/local/4[01;31m[K80[m[K54.py

MyVideoConverter Pro 3.14 - 'Output Folder' Buffer Overflow
| windows/local/4[01;31m[K80[m[K55.py

MyVideoConverter Pro 3.14 - 'TVSeries' Buffer Overflow
| windows/local/4[01;31m[K80[m[K56.py

MyWebServer 1.0.3 - Denial of Service
| windows/dos/175[01;31m[K80[m[K.py

Nanometrics Centaur 4.3.23 - Unauthenticated Remote Memory Leak
| hardware/webapps/4[01;31m[K80[m[K98.py

Native Instruments Traktor Pro 1.2.6 - Stack Buffer Overflow (PoC)
| windows/dos/155[01;31m[K80[m[K.pl

NaviCOPA Web Server 2.0.1 - URL Handling Buffer Overflow (Metasploit)
| windows/remote/16[01;31m[K80[m[K8.rb

nensor CMS 2.01 - Multiple Vulnerabilities
| php/webapps/11[01;31m[K80[m[K6.txt

NetcPlus BrowseGate 2.[01;31m[K80[m[K - Denial of Service
| windows/dos/20233.txt

NetcPlus BrowseGate 2.[01;31m[K80[m[K.2 - Weak Encryption
| windows/local/20409.c

Netgear SSL312 Router - Denial of Service
| hardware/dos/[01;31m[K80[m[K08.txt

Netgear WiFi Router JWNR2010v5 / R60[01;31m[K80[m[K - Authentication
Bypass                                                  |
hardware/webapps/47117.txt

Netgear Wireless Management System 2.1.4.15 (Build 1236) - Privilege
Escalation                                |
hardware/webapps/3[01;31m[K80[m[K97.txt

NethServer 7.3.1611 - Cross-Site Request Forgery (Create User / Enable
SSH Access)                               |
json/webapps/425[01;31m[K80[m[K.html

Netlink XPON 1GE WiFi V2[01;31m[K80[m[K1RGW - Remote Command Execution
| hardware/webapps/48470.txt
```

NetPCLinker 1.0.0.0 - Buffer Overflow (SEH Egghunter)
| windows/local/486[01;31m[K80[m[K.py

NetVault: SmartDisk 1.2 - 'libnvbasics.dll' Remote Denial of Service
| windows/dos/35[01;31m[K80[m[K4.txt

NetVIOS 2.0 - 'page.asp' SQL Injection
| asp/webapps/27[01;31m[K80[m[K.txt

News Script PHP 1.2 - Multiple Vulnerabilities
| php/webapps/191[01;31m[K80[m[K.txt

Newsgrab 0.5.0pre4 - Multiple Local/Remote Vulnerabilities
| linux/remote/250[01;31m[K80[m[K.txt

NextAge Cart - 'index.php' Multiple Cross-Site Scripting
Vulnerabilities |
php/webapps/285[01;31m[K80[m[K.txt

Nfdump Nfcapd 1.6.14 - Multiple Vulnerabilities
| linux/dos/39[01;31m[K80[m[K0.txt

Nginx 0.6.36 - Directory Traversal
| multiple/remote/12[01;31m[K80[m[K4.txt

NJStar Communicator 3.00 - MiniSMTP Server Remote (Metasploit)
| windows/remote/1[01;31m[K80[m[K57.rb

Nokia N95-8 - '.jpg' Remote Crash (PoC)
| hardware/dos/[01;31m[K80[m[K13.txt

Nokia N95-8 browser - 'setAttributeNode' Method Crash
| hardware/dos/[01;31m[K80[m[K51.html

Nokia PC Suite Video Manager 7.1.1[01;31m[K80[m[K.64 - '.mp4' Denial of
Service | windows/dos/18795.py

NoMachine < 6.0.[01;31m[K80[m[K (x64) - 'nxfuse' Privilege Escalation
| windows_x86-64/local/44168.py

NoMachine < 6.0.[01;31m[K80[m[K (x86) - 'nxfuse' Privilege Escalation
| windows_x86/local/44167.c

Nortel CVX 1[01;31m[K80[m[K0 Multi-Service Access Switch - Default SNMP
Community |
hardware/remote/21378.txt

NoseRub 0.5.2 - Login SQL Injection
| php/webapps/4[01;31m[K80[m[K5.txt

Novaboard 1.0.0 - Multiple Vulnerabilities
| php/webapps/[01;31m[K80[m[K63.txt

```
Novell Groupwise 8.0 - Multiple Remote Vulnerabilities
| novell/dos/349[01;31m[K80[m[K.py

NPDS 5.10 - Multiple Input Validation Vulnerabilities
| php/webapps/2[01;31m[K80[m[K06.txt

NSClient++ 0.5.2.35 - Privilege Escalation
| windows/local/46[01;31m[K80[m[K2.txt

ntop-ng 2.5.160[01;31m[K80[m[K5 - Username Enumeration
| multiple/webapps/40942.py

ntop-ng < 3.4.1[01;31m[K80[m[K617 - Authentication Bypass
| lua/webapps/44973.py

NTP 4.2.8p8 - Denial of Service
| linux/dos/40[01;31m[K80[m[K6.py

Nullsoft Winamp 2.[01;31m[K80[m[K - Automatic Update Check Buffer
Overflow                                                  |
windows/remote/21595.c

Nuts CMS - PHP Remote Code Injection / Execution
| php/webapps/37[01;31m[K80[m[K9.php

OCS Inventory NG 2.0.1 - Persistent Cross-Site Scripting
| windows/webapps/1[01;31m[K80[m[K05.txt

Olicom XLT-F XL [01;31m[K80[m[K IM V5.5BL2 - Undocumented Community
String                                                    |
hardware/remote/20892.txt

Omni-Secure - 'dir' Multiple File Disclosure Vulnerabilities
| php/webapps/3[01;31m[K80[m[K25.txt

online Chatting System 1.0 - 'id' SQL Injection
| php/webapps/484[01;31m[K80[m[K.txt

Online Guestbook Pro 5.1 - 'ogp_show.php' Cross-Site Scripting
| php/webapps/34[01;31m[K80[m[K3.txt

Online Job Portal 1.0 - 'user_email' SQL Injection
| php/webapps/4[01;31m[K80[m[K07.txt

Online Job Portal 1.0 - Cross Site Request Forgery (Add User)
| php/webapps/4[01;31m[K80[m[K16.txt

Online Job Portal 1.0 - Remote Code Execution
| php/webapps/4[01;31m[K80[m[K12.txt

Online Quiz System - 'prequiz.asp?exam' Cross-Site Scripting
| asp/webapps/274[01;31m[K80[m[K.txt
```

```
Online store PHP script - Multiple Cross-Site Scripting / SQL
Injections                                    |
php/webapps/354[01;31m[K80[m[K.txt

Online Subtitles Workshop - Cross-Site Scripting
| php/webapps/1[01;31m[K80[m[K35.txt

Open Constructor - 'confirm.php?q' Cross-Site Scripting
| php/webapps/375[01;31m[K80[m[K.txt

Open Educational System 0.1 Beta - 'CONF_INCLUDE_PATH' Multiple Remote
File Inclusions                        |
php/webapps/336[01;31m[K80[m[K.txt

Open-Realty 2.5.8 - Cross-Site Request Forgery
| php/webapps/3[01;31m[K80[m[K37.html

OpenAM 13.0 - LDAP Injection
| java/webapps/504[01;31m[K80[m[K.go

OpenBiz Cubi Lite 3.0.8 - 'username' SQL Injection
| php/webapps/45[01;31m[K80[m[K1.txt

OpenBSD - Dynamic Loader chpass Privilege Escalation (Metasploit)
| openbsd/local/47[01;31m[K80[m[K3.rb

OpenBSD 4.x - Portmap Remote Denial of Service
| bsd/dos/3[01;31m[K80[m[K59.c

OpenBSD 6.x - Dynamic Loader Privilege Escalation
| openbsd/local/477[01;31m[K80[m[K.txt

OpenCart 1.5.1.2 - Blind SQL Injection
| php/webapps/17[01;31m[K80[m[K7.txt

OpenEMM-2013 8.10.3[01;31m[K80[m[K.hf13.0.066 - SOAP SQL Injection /
Persistent Cross-Site Scripting                    |
jsp/webapps/27187.py

Openfire 3.6.2 - 'log.jsp' Directory Traversal
| jsp/webapps/326[01;31m[K80[m[K.txt

OpenPLC 3 - Remote Code Execution (Authenticated)
| python/webapps/49[01;31m[K80[m[K3.py

openSIS 5.1 - 'ajax.php' Local File Inclusion
| php/webapps/3[01;31m[K80[m[K39.txt

openSIS 9.1 - SQLi (Authenticated)
| php/webapps/520[01;31m[K80[m[K.txt

OpenSLP 2.0.0 - Multiple Vulnerabilities
| linux/local/45[01;31m[K80[m[K4.txt
```

```
OpenSMTPD - MAIL FROM Remote Code Execution (Metasploit)
| linux/remote/4[01;31m[K80[m[K38.rb

OpenSMTPD 6.4.0 < 6.6.1 - Local Privilege Escalation + Remote Code
Execution                                 |
openbsd/remote/4[01;31m[K80[m[K51.pl

OpenTFTP 1.66 - Local Privilege Escalation
| windows/local/4[01;31m[K80[m[K60.txt

Opera 11.51 - Use-After-Free Crash (PoC)
| windows/dos/1[01;31m[K80[m[K14.html

Opera 11.52 - Denial of Service (PoC)
| windows/dos/1[01;31m[K80[m[K06.html

Opera 11.52 - Stack Overflow
| windows/dos/1[01;31m[K80[m[K08.html

Opera 9 IRC Client - Remote Denial of Service
| multiple/dos/21[01;31m[K80[m[K.py

Opera 9.60 - Persistent Cross-Site Scripting
| windows/remote/6[01;31m[K80[m[K1.txt

Opera 9.61 - 'opera:historysearch' Code Execution
| windows/remote/68[01;31m[K80[m[K.html

Opial 1.0 - 'albumID' SQL Injection
| php/webapps/90[01;31m[K80[m[K.txt

Opial CMS 2.0 - Multiple Vulnerabilities
| php/webapps/18[01;31m[K80[m[K3.txt

Optoma 10[01;31m[K80[m[KPSTX Firmware C02 - Authentication Bypass
| hardware/remote/51444.txt

Optus/Huawei E960 HSDPA Router - Sms Cross-Site Scripting
| hardware/remote/[01;31m[K80[m[K96.txt

Oracle - Document Capture BlackIce DEVMODE
| windows/remote/9[01;31m[K80[m[K5.html

Oracle - xdb.xdb_pitrig_pkg.PITRIG_DROPMETADATA procedure
| windows/remote/1[01;31m[K80[m[K93.txt

Oracle 10g - MDSYS.SDO_TOPO_DROP_FTBL SQL Injection (Metasploit)
| multiple/local/[01;31m[K80[m[K74.rb

Oracle 11.1 - Database Network Foundation Heap Memory Corruption
| multiple/dos/330[01;31m[K80[m[K.txt
```

```
Oracle 8 Server - 'TNSLSNR[01;31m[K80[m[K.EXE' Denial of Service
| windows/dos/20779.pl

Oracle 8i - TNS Listener Buffer Overflow
| windows/remote/209[01;31m[K80[m[K.c

Oracle 9i XDB (Windows x86) - HTTP PASS Overflow (Metasploit)
| windows_x86/remote/16[01;31m[K80[m[K9.rb

Oracle 9i XDB 9.2.0.1 - HTTP PASS Buffer Overflow
| windows/remote/427[01;31m[K80[m[K.py

Oracle AutoVue 20.0.1 AutoVueX - ActiveX Control SaveViewStateToFile
| windows/remote/1[01;31m[K80[m[K16.txt

Oracle DataDirect - Multiple Native Wire Protocol ODBC Drivers HOST
Attribute Stack Buffer Overflows (PoC) |
windows/dos/1[01;31m[K80[m[K07.txt

Oracle DataDirect ODBC Drivers - HOST Attribute 'arsqls24.dll' Stack
Buffer Overflow (PoC)                 |
windows/dos/1[01;31m[K80[m[K52.php

Oracle GlassFish Server 2.1.1/3.0.1 - Multiple Subcomponent Resource
Identifier Traversal Arbitrary File A |
multiple/remote/38[01;31m[K80[m[K2.txt

Oracle Hyperion Financial Management TList6 - ActiveX Control Remote
Code Execution                        |
windows/remote/1[01;31m[K80[m[K62.txt

Oracle Hyperion Strategic Finance 12.x - Tidestone Formula One WorkBook
OLE Control TTF16.ocx Remote Heap  |
windows/remote/1[01;31m[K80[m[K92.html

Oracle Java lookUpByteBI - Heap Buffer Overflow
| windows/dos/2[01;31m[K80[m[K50.txt

Oracle Web Listener 4.0.x - for NT Batch File
| windows/remote/19[01;31m[K80[m[K9.txt

Oracle Weblogic 10.3.6.0.0 / 12.1.3.0.0 - Remote Code Execution
| windows/webapps/467[01;31m[K80[m[K.py

Oracle WebLogic Server 10.3.6.0 - Java Deserialization Remote Code
Execution                             |
java/remote/42[01;31m[K80[m[K6.py

Oracle XDB FTP Service - UNLOCK Buffer Overflow
| windows/remote/[01;31m[K80[m[K.c

OrangeHRM - 'sortField' SQL Injection
| php/webapps/3[01;31m[K80[m[K11.txt
```

```
OrangeHRM 2.6.11 - 'lib/controllers/CentralController.php' URI Cross-
Site Scripting                          |
php/webapps/363[01;31m[K80[m[K.txt

OrderSys 1.6.4 - SQL Injection
| php/webapps/1[01;31m[K80[m[K91.txt

osCommerce Online Merchant 2.2 - File Disclosure / Authentication
Bypass                                    |
php/webapps/12[01;31m[K80[m[K1.txt

osCSS2 - '_ID' Local file Inclusion
| php/webapps/1[01;31m[K80[m[K99.txt

Osmodia Bulletin Board 1.x - 'admin.txt' File Disclosure
| php/webapps/[01;31m[K80[m[K88.txt

OSSIM 2.1.5 - Remote Command Execution
| php/webapps/104[01;31m[K80[m[K.txt

osTicket 1.6 RC5 - Multiple Vulnerabilities
| php/webapps/113[01;31m[K80[m[K.txt

OtomiGen.x 2.2 - 'lang' Local File Inclusion
| php/webapps/56[01;31m[K80[m[K.txt

Pacheckbook 1.1 - 'index.php' Multiple SQL Injections
| php/webapps/27[01;31m[K80[m[K8.txt

PackWeb Formap E-learning 1.0 - 'NumCours' SQL Injection
| php/webapps/4[01;31m[K80[m[K24.txt

Palm WebOS 1.0/1.1 - 'LunaSysMgr' Service Denial of Service
| hardware/dos/332[01;31m[K80[m[K.txt

Palo Alto Traps Server 3.1.2.1546 - Persistent Cross-Site Scripting
| windows/webapps/365[01;31m[K80[m[K.rb

Pandora Fms - SQL Injection Remote Code Execution (Metasploit)
| php/remote/353[01;31m[K80[m[K.rb

Pandora FMS 7.0NG - 'net_tools.php' Remote Code Execution
| php/webapps/482[01;31m[K80[m[K.py

PANDORAFMS 7.0 - Authenticated Remote Code Execution
| php/webapps/4[01;31m[K80[m[K64.py

Papoo CMS 3.x - 'pfadhier' Local File Inclusion
| php/webapps/[01;31m[K80[m[K30.txt

part-db 0.5.11 - Remote Code Execution (RCE)
| php/webapps/50[01;31m[K80[m[K0.sh
```

```
Pavuk Digest - Authentication Remote Buffer Overflow
| linux/remote/3[01;31m[K80[m[K.c

PCMan FTP Server 2.0.7 - 'GET' Remote Buffer Overflow
| windows/remote/3[01;31m[K80[m[K03.py

PCMan FTP Server 2.0.7 - 'RENAME' Remote Buffer Overflow
| windows/remote/3[01;31m[K80[m[K13.py

PCMan FTP Server 2.0.7 - 'UMASK' Remote Buffer Overflow
| windows/remote/406[01;31m[K80[m[K.py

Pegasi Web Server 0.2.2 - Arbitrary File Access
| linux/remote/23[01;31m[K80[m[K2.txt

Pegasi Web Server 0.2.2 - Error Page Cross-Site Scripting
| linux/remote/23[01;31m[K80[m[K3.txt

PerlCal 2.x - Directory Traversal
| cgi/remote/20[01;31m[K80[m[K8.txt

Persits Software XUpload Control - 'AddFolder()' Remote Buffer Overflow
| windows/remote/4[01;31m[K80[m[K6.html

PFTP Server 8.0f Lite - textfield Local Buffer Overflow (SEH) (PoC)
| windows/dos/3[01;31m[K80[m[K28.pl

PG Social Networking - Arbitrary File Upload
| php/webapps/142[01;31m[K80[m[K.txt

philboard 1.02 - SQL Injection
| php/webapps/11[01;31m[K80[m[K2.txt

Philips VOIP841 Firmware 1.0.4.[01;31m[K80[m[K0 - Multiple
Vulnerabilities                                                 |
hardware/remote/5113.txt

pHNews Alpha 1 - 'genbackup.php' Database Disclosure
| php/webapps/[01;31m[K80[m[K73.txt

pHNews Alpha 1 - 'mod' SQL Injection
| php/webapps/[01;31m[K80[m[K72.txt

Phorum < 5.0.3 Beta - Cross Site Scripting
| php/webapps/43[01;31m[K80[m[K2.txt

phosheezy 2.0 - Remote Command Execution
| php/webapps/77[01;31m[K80[m[K.pl

PhotoPost < 4.6 - Multiple Vulnerabilities
| php/webapps/43[01;31m[K80[m[K8.txt
```

```
PHP 4.x/5.0 - 'Strip_Tags()' Function Bypass
| php/remote/242[01;31m[K80[m[K.txt

PHP 5.1.6 - 'Imap_Mail_Compose()' Remote Buffer Overflow
| php/remote/29[01;31m[K80[m[K7.php

PHP 5.1.6 - 'Msg_Receive()' Memory Allocation Integer Overflow
| php/remote/29[01;31m[K80[m[K8.php

PHP 5.2.0/5.2.1 - Rejected Session ID Double-Free
| linux/local/34[01;31m[K80[m[K.php

PHP 5.2.1 - 'Session.Save_Path()' TMPDIR open_basedir Restriction
Bypass                                  |
php/local/29[01;31m[K80[m[K1.php

PHP 5.2.1 - Multiple functions 'Reference' Information Disclosures
| php/local/29[01;31m[K80[m[K4.php

PHP 5.2.3 'Tidy' Extension - Local Buffer Overflow
| windows/local/40[01;31m[K80[m[K.php

PHP 7.0 < 7.4 (Unix) - 'debug_backtrace' disable_functions Bypass
| php/local/4[01;31m[K80[m[K72.php

PHP Blue Dragon CMS 2.9.1 - Multiple Remote File Inclusions
| php/webapps/2[01;31m[K80[m[K98.txt

PHP Director 0.21 - Remote Command Execution
| php/webapps/[01;31m[K80[m[K14.pl

PHP Event Calendar 4.2 - SQL Injection
| php/webapps/2[01;31m[K80[m[K88.txt

PHP Help Agent 1.1 - 'content' Local File Inclusion
| php/webapps/60[01;31m[K80[m[K.txt

PHP JOBWEBSITE PRO - 'JobSearch3.php' SQL Injection
| php/webapps/5[01;31m[K80[m[K7.txt

PHP Krazy Image Host Script 1.01 - 'id' SQL Injection
| php/webapps/[01;31m[K80[m[K46.txt

PHP Photo Album 0.4.1.16 - Multiple Disclosure Vulnerabilities
| php/webapps/1[01;31m[K80[m[K45.txt

PHP Point Of Sale - 'ofc_upload_image.php' Remote Code Execution
| php/remote/38[01;31m[K80[m[K9.php

PHP Property Rental Script - SQL Injection / Cross-Site Scripting
| php/webapps/13[01;31m[K80[m[K5.txt
```

PHP Proxy 3.0.3 - Local File Inclusion
| php/webapps/457[01;31m[K80[m[K.py

PHP Real Estate Script - SQL Injection
| php/webapps/13[01;31m[K80[m[K2.txt

PHP-Fusion 6.1.5 Mod Calendar_Panel - 'Show_Event.php' SQL Injection
| php/webapps/29[01;31m[K80[m[K6.pl

PHP-Fusion Mod avatar_studio - Local File Inclusion
| php/webapps/10[01;31m[K80[m[K8.txt

PHP-Nuke 'KuiraniKerim' Module - 'sid' SQL Injection
| php/webapps/31[01;31m[K80[m[K5.txt

PHP-Nuke 6.x - 'Category' SQL Injection
| php/webapps/236[01;31m[K80[m[K.php

PHP-Nuke 7.4 - Admin
| php/webapps/[01;31m[K80[m[K1.c

PHP-Sugar 0.[01;31m[K80[m[K - 'index.php?t' Local File Inclusion
| php/webapps/9036.txt

PHPAccess - SQL Injection
| php/webapps/13[01;31m[K80[m[K3.txt

phpAuthent 0.2.1 - SQL Injection
| php/webapps/11[01;31m[K80[m[K1.txt

PHPBandManager 0.8 - 'index.php?pg' Remote File Inclusion
| php/webapps/3[01;31m[K80[m[K2.txt

phpBazar 2.0.2 - 'adid' SQL Injection
| php/webapps/62[01;31m[K80[m[K.txt

phpBazar 2.1.0 - Remote File Inclusion / Authentication Bypass
| php/webapps/1[01;31m[K80[m[K4.txt

phpBB - 'BBRSS.php' Remote File Inclusion
| php/webapps/2[01;31m[K80[m[K24.txt

phpBB 2.0.15 - 'highlight' Database Authentication Details
| php/webapps/10[01;31m[K80[m[K.pl

phpBB 2.0.20 - Admin/Restore DB/default_lang Remote Command Execution
| php/webapps/17[01;31m[K80[m[K.php

phpBB 3 - 'autopost bot mod 0.1.3' Remote File Inclusion
| php/webapps/[01;31m[K80[m[K83.txt

phpBB < 2.0.6d - Cross Site Scripting
| php/webapps/43[01;31m[K80[m[K1.txt

```
phpBB < 2.0.7a - Multiple Vulnerabilities
| php/webapps/43[01;31m[K80[m[K5.txt

phpBB Add Name Module - 'Not_Mem.php' Remote File Inclusion
| php/webapps/28[01;31m[K80[m[K4.pl

phpBB Security Suite Mod 1.0.0 - 'logger_engine.php' Remote File
Inclusion                                  |
php/webapps/24[01;31m[K80[m[K.txt

PHPbbBook 1.3 - 'bbcode.php?l' Local File Inclusion
| php/webapps/79[01;31m[K80[m[K.pl

phpBugTracker 1.0.3 - Authentication Bypass
| php/webapps/8[01;31m[K80[m[K8.txt

phpcrs 2.06 - 'importFunction' Local File Inclusion
| php/webapps/6[01;31m[K80[m[K6.txt

phpFaber CMS 2.0.5 - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/342[01;31m[K80[m[K.txt

phpGB 1.1 - HTML Injection
| php/webapps/217[01;31m[K80[m[K.txt

PHPKF Forum 1.[01;31m[K80[m[K - 'profil_degistir.php' Cross-Site
Request Forgery                                          |
php/webapps/15685.html

phpLDAPadmin 0.9.4b - Denial of Service
| php/dos/1[01;31m[K80[m[K23.java

phpLDAPadmin 1.2.1.1 - Remote PHP Code Injection (1)
| php/webapps/1[01;31m[K80[m[K21.php

phpLDAPadmin 1.2.1.1 - Remote PHP Code Injection (Metasploit) (2)
| php/webapps/1[01;31m[K80[m[K31.rb

PHPLinks 2.1.2 - Add Site HTML Injection
| php/webapps/221[01;31m[K80[m[K.txt

phpListPro 2.0.1 - 'Language' Remote Code Execution
| php/webapps/1[01;31m[K80[m[K5.pl

phpMyChat Plus 1.98 - 'pmc_username' SQL Injection
| php/webapps/4[01;31m[K80[m[K66.txt

phpMyDirectory 10.4.4 - 'ROOT_PATH' Remote File Inclusion
| php/webapps/1[01;31m[K80[m[K8.txt

PHPMyFAQ 2.7.0 - 'ajax_create_folder.php' Remote Code Execution
| php/webapps/1[01;31m[K80[m[K84.php
```

```
phpMyFAQ 2.8.x - Multiple Vulnerabilities
| php/webapps/345[01;31m[K80[m[K.txt

phpMyRealty 2.0.0 - 'location' SQL Injection
| php/webapps/61[01;31m[K80[m[K.txt

PHPNews 1.2.3/1.2.4 - 'auth.php' Remote File Inclusion
| php/webapps/251[01;31m[K80[m[K.py

PHPOracleView - 'include_all.inc.php?page_dir' Remote File Inclusion
| php/webapps/3[01;31m[K80[m[K3.txt

phpScheduleIt 1.2.10 - 'reserve.php' Arbitrary Code Injection
(Metasploit)                                  |
php/webapps/1[01;31m[K80[m[K37.rb

phpscripte24 Niedrig Gebote Pro Auktions System II - Blind SQL
Injection                                     |
php/webapps/11[01;31m[K80[m[K5.txt

PHPSlideShow 0.9.9 - 'Directory' Cross-Site Scripting
| php/webapps/30[01;31m[K80[m[K6.txt

PHPUserBase 1.3b - 'unverified.inc.php' Remote File Inclusion
| php/webapps/51[01;31m[K80[m[K.txt

PhpWiki 1.5.4 - Multiple Vulnerabilities
| php/webapps/3[01;31m[K80[m[K27.txt

phpYabs 0.1.2 - 'Azione' Remote File Inclusion
| php/webapps/[01;31m[K80[m[K05.txt

PicMe 2.1.0 - Arbitrary File Upload
| php/webapps/10[01;31m[K80[m[K2.txt

PinApp Mail-SeCure 3.70 - Access Control Failure
| linux/local/286[01;31m[K80[m[K.txt

Ping IP - Authentication Bypass
| asp/webapps/7[01;31m[K80[m[K3.txt

Pinnacle Cart 3.3 - 'index.php' Cross-Site Scripting
| php/webapps/27[01;31m[K80[m[K0.txt

PixelStor 5000 K:4.0.15[01;31m[K80[m[K-20150629 - Remote Code Execution
| php/webapps/47899.py

PlayJoom 0.10.1 - 'catid' SQL Injection
| php/webapps/45[01;31m[K80[m[K3.txt

PLC Wireless Router GPN2.4P21-C-CN - Incorrect Access Control
| hardware/webapps/465[01;31m[K80[m[K.txt
```

```
Pluck CMS 4.7.3 - Multiple Vulnerabilities
| php/webapps/3[01;31m[K80[m[K02.txt

pMachine 1.0/2.x - '/lib/' Multiple Script Direct Request Full Path
Disclosures                              |
php/webapps/22[01;31m[K80[m[K8.txt

pMachine 1.0/2.x - Multiple Script 'sfx' Full Path Disclosures
| php/webapps/22[01;31m[K80[m[K9.txt

Poison Ivy 2.3.2 - Remote Buffer Overflow
| windows/remote/35[01;31m[K80[m[K6.c

Poppler 0.10.3 - Denial of Service
| linux/dos/32[01;31m[K80[m[K0.txt

Postfix 2.6-200[01;31m[K80[m[K814 - 'symlink' Local Privilege
Escalation                                                  |
linux/local/6337.sh

Postfix < 2.4.9/2.5.5/2.6-200[01;31m[K80[m[K902 - '.forward' Local
Denial of Service                                    |
multiple/dos/6472.c

PostNuke PostWrap Module - Remote File Inclusion / Code Execution
| php/webapps/[01;31m[K80[m[K0.txt

Potato News 1.0.0 - Local File Inclusion
| php/webapps/[01;31m[K80[m[K32.txt

PotPlayer 1.5.39036 - '.wav' Crash (PoC)
| windows/dos/2[01;31m[K80[m[K51.py

Power Phlogger 2.2.x - Cross-Site Scripting
| php/webapps/333[01;31m[K80[m[K.txt

Power Tab Editor 1.7 (Build [01;31m[K80[m[K) - Local Buffer Overflow
| windows/local/13820.pl

Power Up HTML 0.[01;31m[K80[m[K33 Beta - Directory Traversal Arbitrary
File Disclosure                                | cgi/remote/21102.txt

Power/Personal FTP Server - RETR Denial of Service
| windows/dos/143[01;31m[K80[m[K.py

powermovielist 0.14b - SQL Injection / Cross-Site Scripting
| php/webapps/[01;31m[K80[m[K62.txt

PowerScripts PlusMail WebConsole 1.0 - Weak Authentication (2)
| cgi/remote/20[01;31m[K80[m[K0.c

PowerScripts PlusMail WebConsole 1.0 - Weak Authentication (3)
| cgi/remote/20[01;31m[K80[m[K1.c
```

```
pPIM 1.01 - 'notes.php' Remote Command Execution
| php/webapps/[01;31m[K80[m[K93.pl

Pre ADS Portal 2.0 - SQL Injection
| php/webapps/5[01;31m[K80[m[K4.txt

Pre Job Board - 'JobSearch.php' SQL Injection
| php/webapps/5[01;31m[K80[m[K9.txt

Pre News Manager 1.0 - 'id' SQL Injection
| php/webapps/5[01;31m[K80[m[K3.txt

Pre Studio Business Cards Designer - SQL Injection
| asp/webapps/1[01;31m[K80[m[K09.txt

Prime95 Version 29.8 build 6 - Buffer Overflow (SEH)
| windows/local/47[01;31m[K80[m[K2.py

Prinect Archive System 2015 Release 2.6 - Cross-Site Scripting
| multiple/webapps/46[01;31m[K80[m[K4.txt

Private Internet Access 3.3 - 'pia-service' Unquoted Service Path
| windows/local/50[01;31m[K80[m[K4.txt

PrivateTunnel Client 2.7.0 (x64) - Local Credentials Disclosure
| windows_x86-64/local/403[01;31m[K80[m[K.py

PrivateWire Gateway 3.7 (Windows x86) - Remote Buffer Overflow
(Metasploit)                                    |
windows_x86/remote/26[01;31m[K80[m[K.pm

ProArcadeScript to Game - SQL Injection
| php/webapps/110[01;31m[K80[m[K.txt

Procps-ng - Multiple Vulnerabilities
| linux/local/44[01;31m[K80[m[K6.txt

ProFTPd - 'mod_mysql' Authentication Bypass
| multiple/remote/[01;31m[K80[m[K37.txt

ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution
| linux/remote/36[01;31m[K80[m[K3.py

ProjeQtOr Project Management Tool 7.2.5 - Remote Code Execution
| php/webapps/456[01;31m[K80[m[K.txt

Prometeo 1.0.65 - SQL Injection
| php/webapps/14[01;31m[K80[m[K6.txt

ProShow 9.0.3797 - Local Privilege Escalation
| windows/local/469[01;31m[K80[m[K.py
```

```
Protector Plus AntiVirus 8/9 - Local Privilege Escalation
| windows/local/96[01;31m[K80[m[K.txt

Prozilla 1.3.7.3 - Remote Format String
| linux/remote/[01;31m[K80[m[K6.c

PTC Site's - Remote Code Execution / Cross-Site Scripting
| php/webapps/12[01;31m[K80[m[K8.txt

PulseAudio 0.9.5 - 'Assert()' Remote Denial of Service
| linux/dos/29[01;31m[K80[m[K9.txt

PunBB Automatic Image Upload 1.3.5 - Arbitrary File Delete
| php/webapps/92[01;31m[K80[m[K.pl

PyCrypto ARC2 Module - Remote Buffer Overflow
| linux/remote/327[01;31m[K80[m[K.py

Pyrophobia 2.1.3.1 - Local File Inclusion Command Execution
| php/webapps/[01;31m[K80[m[K95.pl

Q-News 2.0 - Remote Command Execution
| php/webapps/[01;31m[K80[m[K31.pph

Qto File Manager 1.0 - 'index.php' Cross-Site Scripting
| php/webapps/2[01;31m[K80[m[K64.txt

Quagga Routing Software Suite 0.9x - RIPd RIPv1 Request Routing Table
Disclosure                          |
linux/remote/27[01;31m[K80[m[K1.txt

Quagga Routing Software Suite 0.9x - RIPd RIPv1 RESPONSE Packet Route
Injection                           |
linux/remote/27[01;31m[K80[m[K2.txt

Qualcomm Eudora 5 - MIME MultiPart Boundary Buffer Overflow
| windows/remote/216[01;31m[K80[m[K.pl

quality point 1.0 newsfeed - SQL Injection / Cross-Site Scripting
| php/webapps/11[01;31m[K80[m[K8.txt

Quick Classifieds 1.0 - 'locate.php3?DOCUMENT_ROOT' Remote File
Inclusion                                    |
php/webapps/314[01;31m[K80[m[K.txt

QuickDate 1.3.2 - SQL Injection
| php/webapps/4[01;31m[K80[m[K22.txt

R 3.4.4 - Local Buffer Overflow (DEP Bypass)
| windows_x86/local/446[01;31m[K80[m[K.py

RAD SecFlow-1v SF_0290_2.3.01.26  - Persistent Cross-Site Scripting
| hardware/webapps/48[01;31m[K80[m[K7.txt
```

RAD SecFlow-1v SF_0290_2.3.01.26 - Cross-Site Request Forgery (Reboot)
| hardware/webapps/48[01;31m[K80[m[K9.txt

RadScripts RadLance 7.0 - 'popup.php' Local File Inclusion
| php/webapps/278[01;31m[K80[m[K.pl

RahnemaCo - 'page.php' PageID Remote File Inclusion
| php/webapps/2[01;31m[K80[m[K48.txt

RahnemaCo - 'page.php' Remote File Inclusion
| php/webapps/2[01;31m[K80[m[K25.txt

RaidenFTPd 2.1 - Directory Traversal
| windows/remote/20[01;31m[K80[m[K3.txt

Raisecom XPON ISCOMHT[01;31m[K80[m[K3G-U_2.0.0_140521_R4.1.47.002 - Remote Code Execution |
hardware/webapps/46489.txt

Rankem - File Disclosure / Cross-Site Scripting / Cookie
| php/webapps/7[01;31m[K80[m[K5.txt

Rapid7 Nexpose Installer 6.6.39 - 'nexposeengine' Unquoted Service Path
| windows/local/48[01;31m[K80[m[K8.txt

Rapidsendit Clone Script - 'admin.php' Insecure Cookie Authentication Bypass |
php/webapps/34[01;31m[K80[m[K8.txt

RAR Password Recovery 1.[01;31m[K80[m[K - 'User Name and Registration Code' Denial of Service |
windows/dos/47285.py

RarmaRadio 2.72.4 - 'server' Denial of Service (PoC)
| windows/dos/4[01;31m[K80[m[K15.py

RarmaRadio 2.72.4 - 'username' Denial of Service (PoC)
| windows/dos/4[01;31m[K80[m[K14.py

ravennuke 2.3.0 - Multiple Vulnerabilities
| php/webapps/[01;31m[K80[m[K68.txt

Rentventory - 'index.php' Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/34[01;31m[K80[m[K4.txt

Reptile Rootkit - reptile_cmd Privilege Escalation (Metasploit)
| linux/local/47[01;31m[K80[m[K4.rb

Research In Motion BlackBerry Device Software 4.7.1 - Cross Domain Information Disclosure |
hardware/remote/34[01;31m[K80[m[K2.html

Resumes Management and Job Application Website 1.0 - RCE (Unauthenticated) | php/webapps/493[01;31m[K80[m[K.txt

RichFX Basic Player 1.1 - ActiveX Control Multiple Buffer Overflow Vulnerabilities | windows/dos/30[01;31m[K80[m[K5.html

Ricoh DC (SR10) 1.1.0.8 - Denial of Service | windows/dos/3[01;31m[K80[m[K52.py

Ricoh Driver - Privilege Escalation (Metasploit) | windows/local/4[01;31m[K80[m[K36.rb

RICOH MP C1[01;31m[K80[m[K3 JPN Printer - Cross-Site Scripting | hardware/webapps/45526.txt

RobTex Viking Server 1.0.6 Build 355 - Remote Buffer Overflow | windows/remote/201[01;31m[K80[m[K.c

Rocket Servergraph Admin Center - fileRequestor Remote Code Execution (Metasploit) | multiple/remote/33[01;31m[K80[m[K7.rb

Rocket Software UniData 7.2.7.3[01;31m[K80[m[K6 - Denial of Service | windows/dos/15260.txt

Rumba FTP Client 4.2 - PASV Buffer Overflow (SEH) | windows/remote/123[01;31m[K80[m[K.pl

RW-Download 4.0.6 - 'index.php' SQL Injection | php/webapps/160[01;31m[K80[m[K.txt

RXS-3211 IP Camera - UDP Packet Password Information Disclosure | hardware/remote/35[01;31m[K80[m[K0.txt

S-CMS 1.1 Stable - Insecure Cookie Handling / Mass Page Delete | php/webapps/[01;31m[K80[m[K71.txt

S9Y Serendipity Freetag-plugin 3.21 - 'index.php' Cross-Site Scripting | php/webapps/35[01;31m[K80[m[K8.txt

SafeNet Sentinel Protection Server 7.x/Keys Server 1.0.3 - Directory Traversal | windows/remote/30[01;31m[K80[m[K9.txt

Sagemcom F@ST 3864 V2 - Get Admin Password | hardware/webapps/37[01;31m[K80[m[K1.sh

Sam Hawker wmcdplay 1.0 beta1-2 - Local Buffer Overflow (1) | linux/local/19[01;31m[K80[m[K2.c

Sam Hawker wmcdplay 1.0 beta1-2 - Local Buffer Overflow (2)
| linux/local/19[01;31m[K80[m[K3.txt

Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)
| bsd_x86/remote/168[01;31m[K80[m[K.rb

SAMSUNG NET-i Viewer 1.37 - Overwrite (SEH)
| windows/local/18[01;31m[K80[m[K8.html

Samsung SyncThruWeb 2.01.00.26 - SMB Hash Disclosure
| hardware/webapps/3[01;31m[K80[m[K04.txt

SAP Management Console - OSExecute Payload Execution (Metasploit)
| windows/webapps/1[01;31m[K80[m[K32.rb

SAP Sybase Adaptive Server Enterprise - XML External Entity Information Disclosure |
multiple/remote/38[01;31m[K80[m[K5.txt

SaphpLesson 1.1/2.0/3.0 - Multiple SQL Injections
| php/webapps/2[01;31m[K80[m[K59.txt

SAS Hotel Management System - 'id' SQL Injection
| asp/webapps/[01;31m[K80[m[K65.txt

SAS Hotel Management System - Arbitrary File Upload
| asp/webapps/[01;31m[K80[m[K70.txt

Savant Web Server 3.1 - Denial of-Service (PoC)
| windows/dos/3[01;31m[K80[m[K79.py

Savant Web Server 3.1 - GET Universal Remote Overflow
| windows/remote/42[01;31m[K80[m[K.pl

Science Fair In A Box - SQL Injection / Cross-Site Scripting
| php/webapps/13[01;31m[K80[m[K1.txt

SCO Unixware 7.1 - i2odialogd Remote Buffer Overflow
| sco/remote/196[01;31m[K80[m[K.c

Scout Portal Toolkit 1.3.1 - 'SPT-QuickSearch.php' Cross-Site Scripting
| php/webapps/267[01;31m[K80[m[K.txt

ScozNews 1.2.1 - 'mainpath' Remote File Inclusion
| php/webapps/1[01;31m[K80[m[K0.txt

SDFingerD 1.1 - Failure To Drop Privileges Privilege Escalation
| linux/local/22[01;31m[K80[m[K6.sh

Seagull 0.6.3 - 'files' Remote File Disclosure
| php/webapps/49[01;31m[K80[m[K.txt

SearchBlox 8.6.6 - Cross-Site Request Forgery
| java/webapps/44[01;31m[K80[m[K1.txt

SEO Panel 4.8.0 - 'order_col' Blind SQL Injection (2)
| php/webapps/49[01;31m[K80[m[K4.py

Serv-U Web Client 9.0.0.5 - Remote Buffer Overflow (2)
| windows/remote/9[01;31m[K80[m[K0.cpp

SetSeed CMS 5.8.20 - 'loggedInUser' SQL Injection
| php/webapps/1[01;31m[K80[m[K65.txt

SGI IRIX 3/4/5/6 / OpenLinux 1.0/1.1 - routed traceon
| irix/remote/20[01;31m[K80[m[K5.c

SGI IRIX 6.2 - 'fsdump' Local Privilege Escalation
| irix/local/192[01;31m[K80[m[K.txt

ShaadiClone 2.0 - 'addAdminmembercode.php' Arbitrary Add Admin
| php/webapps/8[01;31m[K80[m[K7.html

Shape Web Solutions CMS - SQL Injection
| php/webapps/171[01;31m[K80[m[K.txt

Shareet - 'photo' SQL Injection
| php/webapps/430[01;31m[K80[m[K.txt

ShoreTel Conferencing 19.46.1[01;31m[K80[m[K2.0 - Reflected Cross-Site
Scripting |
php/webapps/49026.txt

SIAP CMS - 'login.asp' SQL Injection
| asp/webapps/291[01;31m[K80[m[K.txt

Siemens SIMATIC S7-300 CPU - Remote Denial of Service
| linux/dos/44[01;31m[K80[m[K2.py

Sienzo Digital Music Mentor 2.6.0.4 - SetEvalExpiryDate Overwrite (SEH)
| windows/remote/38[01;31m[K80[m[K.html

SiliSoftware PHPThumb() 1.7.11-20110[01;31m[K80[m[K81537 -
'/demo/PHPThumb.demo.random.php?dir' Cross-Site Scripting |
php/webapps/37207.txt

SiliSoftware PHPThumb() 1.7.11-20110[01;31m[K80[m[K81537 -
'/demo/PHPThumb.demo.showpic.php?title' Cross-Site Scripting |
php/webapps/37206.txt

SilverNews 2.04 - Authentication Bypass / Local File Inclusion / Remote
Code Execution | php/webapps/[01;31m[K80[m[K04.txt

SilverStripe CMS - Multiple HTML Injection Vulnerabilities
| php/webapps/387[01;31m[K80[m[K.txt

Simbas CMS 2.0 - Authentication Bypass
| php/webapps/83[01;31m[K80[m[K.txt

Simple Free PHP Forum Script - SQL Injection
| php/webapps/1[01;31m[K80[m[K04.txt

Simple Inventory Management System v1.0 - 'email' SQL Injection
| php/remote/51[01;31m[K80[m[K8.txt

simplePms CMS 0.1.4 - Local File Inclusion / Remote Command Execution
| php/webapps/[01;31m[K80[m[K61.pl

Simplog 0.9.3.2 - Multiple Vulnerabilities
| php/webapps/101[01;31m[K80[m[K.txt

Simpnews 2.x - 'Wap_short_news.php' Remote File Inclusion
| php/webapps/2[01;31m[K80[m[K19.txt

Singapore 0.9.x/0.10 - 'index.php?template' Cross-Site Scripting
| php/webapps/2[01;31m[K80[m[K67.txt

Singapore 0.9.x/0.10 - Multiple Traversal Arbitrary File Access
| php/webapps/2[01;31m[K80[m[K66.txt

Sipwise C5 NGCP CSC - 'Multiple' Persistent Cross-Site Scripting (XSS)
| hardware/webapps/49[01;31m[K80[m[K0.html

Sipwise C5 NGCP CSC - Click2Dial Cross-Site Request Forgery (CSRF)
| hardware/webapps/49[01;31m[K80[m[K1.html

SiS Windows VGA Display Manager 6.14.10.3930 - Write-What-Where (PoC)
| windows/dos/3[01;31m[K80[m[K54.txt

Sisfo Kampus 2006 - 'blanko.preview.php' Local File Disclosure
| php/webapps/43[01;31m[K80[m[K.txt

SiteXS CMS 0.1.1 - Arbitrary File Upload / Cross-Site Scripting
| php/webapps/58[01;31m[K80[m[K.txt

SixCMS 6.0 - 'detail.php' Directory Traversal
| php/webapps/2[01;31m[K80[m[K14.txt

SixCMS 6.0 - 'list.php' Cross-Site Scripting
| php/webapps/2[01;31m[K80[m[K13.txt

SkaDate Online 7 - Arbitrary File Upload
| php/webapps/[01;31m[K80[m[K39.txt

Skybluecanvas 1.1-r248 - Cross-Site Request Forgery
| php/webapps/150[01;31m[K80[m[K.txt

SkyFex Client 1.0 - ActiveX 'Start()' Method Remote Stack Overflow
| windows/dos/4[01;31m[K80[m[K1.html

Skype for Linux 2.1 Beta - Multiple Strange Behaviour Vulnerabilities
| linux/remote/109[01;31m[K80[m[K.txt

SMA Solar Technology AG Sunny WebBox device - 1.6 - Cross-Site Request
Forgery |
hardware/webapps/474[01;31m[K80[m[K.txt

Smart ASP Survey - Cross-Site Scripting / SQL Injection
| asp/webapps/138[01;31m[K80[m[K.txt

Smart Search 4.25 - Remote Command Execution
| cgi/webapps/223[01;31m[K80[m[K.pl

SmarterMail 16 - Arbitrary File Upload
| multiple/webapps/485[01;31m[K80[m[K.py

smNews 1.0 - Authentication Bypass / Column Truncation
| php/webapps/[01;31m[K80[m[K76.txt

Snipe Gallery 3.1.4 - 'image.php?image_id' SQL Injection
| php/webapps/26[01;31m[K80[m[K0.txt

Snipe Gallery 3.1.4 - 'search.php?keyword' Cross-Site Scripting
| php/webapps/26[01;31m[K80[m[K1.txt

SnippetMaster Webpage Editor 2.2.2 - Remote File Inclusion / Cross-Site
Scripting | php/webapps/[01;31m[K80[m[K17.txt

SOCA Access Control System 1[01;31m[K80[m[K612 - Cross-Site Request
Forgery (Add Admin) |
php/webapps/46834.txt

SOCA Access Control System 1[01;31m[K80[m[K612 - Information Disclosure
| php/webapps/46832.txt

SOCA Access Control System 1[01;31m[K80[m[K612 - SQL Injection
| php/webapps/46833.txt

SoftBiz Web Hosting Directory Script 1.1 - 'search_result.php?cid' SQL
Injection |
php/webapps/265[01;31m[K80[m[K.txt

SoftBizScripts Dating Script 1.0 - 'featured_photos.php' SQL Injection
| php/webapps/2[01;31m[K80[m[K93.txt

SoftBizScripts Dating Script 1.0 - 'index.php' SQL Injection
| php/webapps/2[01;31m[K80[m[K95.txt

SoftBizScripts Dating Script 1.0 - 'news_desc.php' SQL Injection
| php/webapps/2[01;31m[K80[m[K96.txt

SoftBizScripts Dating Script 1.0 - 'products.php' SQL Injection
| php/webapps/2[01;31m[K80[m[K94.txt

```
Softerra PHP Developer Library 1.5.3 - 'Grid3.lib.php' Remote File
Inclusion                                |
php/webapps/287[01;31m[K80[m[K.txt

SOFTSAURUS 2.01 - Multiple Remote File Inclusions
| php/webapps/11[01;31m[K80[m[K7.txt

Solar FTP Server - Denial of Service
| windows/dos/374[01;31m[K80[m[K.pl

SOPlanning 1.45 - 'by' SQL Injection
| php/webapps/4[01;31m[K80[m[K74.txt

SOPlanning 1.45 - 'users' SQL Injection
| php/webapps/4[01;31m[K80[m[K89.txt

SOPlanning 1.45 - Cross-Site Request Forgery (Add User)
| php/webapps/4[01;31m[K80[m[K86.txt

Soulseek 157 NS - Remote Buffer Overflow (SEH)
| windows/remote/8[01;31m[K80[m[K4.py

SphereFTP Server 2.0 - Crash (PoC)
| windows/dos/3[01;31m[K80[m[K72.py

Splunk 4.3.1 - Denial of Service
| multiple/dos/3[01;31m[K80[m[K38.txt

SportsPHool 1.0 - Remote File Inclusion
| php/webapps/1[01;31m[K80[m[K18.php

SprintWork 2.3.1 - Local Privilege Escalation
| windows/local/4[01;31m[K80[m[K70.txt

SQLiteManager 1.2 - 'main.php' Multiple HTML Injection Vulnerabilities
| php/webapps/296[01;31m[K80[m[K.html

Squid < 3.1 5 - HTTP Version Number Parsing Denial of Service
| multiple/dos/[01;31m[K80[m[K21.pl

Starsgames Control Panel 4.6.2 - 'index.php' Cross-Site Scripting
| php/webapps/31[01;31m[K80[m[K9.txt

Static HTTP Server 1.0 - Denial of Service
| windows/dos/29[01;31m[K80[m[K3.pl

StatsCode - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/34[01;31m[K80[m[K5.txt

Streamcast 0.9.75 - HTTP User-Agent Buffer Overflow (Metasploit)
| windows/remote/16[01;31m[K80[m[K0.rb
```

Student Profile Management System Script 2.0.6 - Authentication Bypass
| php/webapps/439[01;31m[K80[m[K.txt

Sudo 1.8.25p - 'pwfeedback' Buffer Overflow
| linux/local/4[01;31m[K80[m[K52.sh

Sunbird 0.9 - Array Overrun Code Execution
| windows/remote/103[01;31m[K80[m[K.pl

SunShop Shopping Cart 3.5.1 - 'index.php' SQL Injection
| php/webapps/31[01;31m[K80[m[K0.pl

Super Simple Blog Script 2.5.4 - 'entry' SQL Injection
| php/webapps/91[01;31m[K80[m[K.txt

SureMDM On-premise < 6.31 - CAPTCHA Bypass User Enumeration
| multiple/webapps/51[01;31m[K80[m[K4.txt

Surfboard HTTPd 1.1.9 - Remote Buffer Overflow (PoC)
| windows/dos/234[01;31m[K80[m[K.txt

SurfControl Web Filter 4.2.0.1 - File Disclosure
| windows/remote/22[01;31m[K80[m[K7.txt

Sygate Personal Firewall 5.6 build 2[01;31m[K80[m[K8 - ActiveX with DEP
Bypass |
windows/remote/13834.html

Symantec Endpoint Protection 12.1.4023.40[01;31m[K80[m[K - Multiple
Vulnerabilities |
jsp/webapps/35181.txt

Symantec Norton AntiVirus 2002/2003 - Device Driver Memory Overwrite
| windows/local/229[01;31m[K80[m[K.asm

Symantec pcAnywhere 8.0.1/8.0.2/9.0/9.2 - Port Scan Denial of Service
| windows/dos/198[01;31m[K80[m[K.txt

Symantec Sygate Management Server - 'LOGIN' SQL Injection (Metasploit)
| cgi/webapps/16[01;31m[K80[m[K.pm

Symphony 2.2.3 - '/symphony/publish/images?filter' Cross-Site Scripting
| php/webapps/362[01;31m[K80[m[K.txt

Symphony CMS - Local File Inclusion
| php/webapps/12[01;31m[K80[m[K9.txt

Synaccess netBooter NP-0[01;31m[K80[m[K1DU 7.4 - Cross-Site Request
Forgery (Add Admin) |
hardware/webapps/45894.txt

```
Sync Breeze Enterprise 12.4.18 - 'Sync Breeze Enterprise' Unquoted
Service Path                              |
windows/local/4[01;31m[K80[m[K45.txt

Sysax Multi Server 6.40 - SSH Component Denial of Service
| windows/dos/3[01;31m[K80[m[K14.py

TAC Xenta 511/911 - Directory Traversal
| hardware/webapps/44[01;31m[K80[m[K9.txt

Tagit! Tagit2b 2.1.B Build 2 - '/CONFIG/errmsg.inc.php?configpath'
Remote File Inclusion                     |
php/webapps/295[01;31m[K80[m[K.txt

TAGWORX.CMS - 'cid' SQL Injection
| php/webapps/37[01;31m[K80[m[K5.txt

taifajobs 1.0 - 'jobid' SQL Injection
| php/webapps/[01;31m[K80[m[K98.txt

TapinRadio 2.12.3 - 'address' Denial of Service (PoC)
| windows/dos/4[01;31m[K80[m[K11.py

TapinRadio 2.12.3 - 'username' Denial of Service (PoC)
| windows/dos/4[01;31m[K80[m[K13.py

Targem Games Battle Mages 1.0 - Remote Denial of Service
| multiple/dos/23[01;31m[K80[m[K5.txt

TaskInfo 8.2.0.2[01;31m[K80[m[K - Denial of Service (PoC)
| windows/dos/46314.py

Tausch Ticket Script 3 - 'suchauftraege_user.php?userid' SQL Injection
| php/webapps/34[01;31m[K80[m[K9.txt

Tea LaTex 1.0 - Remote Code Execution (Unauthenticated)
| multiple/webapps/48[01;31m[K80[m[K5.txt

Tektronix Phaser 740/750/850/930 - Network Printer Administration
Interface                                 |
hardware/remote/20[01;31m[K80[m[K6.txt

TelnetD encrypt_keyid - Function Pointer Overwrite
| linux/remote/182[01;31m[K80[m[K.c

Tenda W3002R/A302/w309r Wireless Router v5.07.64_en - Remote DNS Change
(PoC)                                     | asp/webapps/443[01;31m[K80[m[K.txt

TFTP Turbo 4.6.1273 - 'TFTP Turbo 4' Unquoted Service Path
| windows/local/4[01;31m[K80[m[K85.txt

The Walking Club - Authentication Bypass
| asp/webapps/7[01;31m[K80[m[K2.txt
```

```
Thecus N4[01;31m[K80[m[K0Eco Nas Server Control Panel - Comand
Injection                                                  |
hardware/webapps/49926.py

ThemeSiteScript 1.0 - 'index.php?loadadminpage' Remote File Inclusion
| php/webapps/47[01;31m[K80[m[K.txt

ThinPrint - 'tpfc.dll' Insecure Library Loading Arbitrary Code
Execution                                      |
windows/local/377[01;31m[K80[m[K.c

Thomson Wireless VoIP Cable Modem TWG850-4B ST9C.05.08 - Authentication
Bypass                                |
hardware/webapps/3[01;31m[K80[m[K67.py

Thyme 1.3 - 'export_to' Local File Inclusion
| php/webapps/[01;31m[K80[m[K29.txt

TightVNC - Authentication Failure Integer Overflow (PoC)
| windows/dos/[01;31m[K80[m[K24.py

Tiki Wiki CMS 15.0 - Arbitrary File Download
| php/webapps/400[01;31m[K80[m[K.txt

TikiWiki < 1.8.1 - Multiple Vulnerabilities
| php/webapps/43[01;31m[K80[m[K9.txt

TinyMCPUK - 'test' Cross-Site Scripting
| php/webapps/3[01;31m[K80[m[K99.txt

Titan FTP Server 3.0 - 'LIST' Denial of Service
| windows/dos/240[01;31m[K80[m[K.pl

Tmax Soft JEUS 3.1.4 p1 - URL.jsp Cross-Site Scripting
| jsp/webapps/22[01;31m[K80[m[K5.txt

ToendaCMS 0.6.1 - 'admin.php' Directory Traversal
| php/webapps/264[01;31m[K80[m[K.txt

Tomabo MP4 Player 3.11.6 - Local Stack Overflow (SEH) (Metasploit)
| windows/local/399[01;31m[K80[m[K.rb

Torrent iPod Video Converter 1.51 - Stack Overflow
| windows/local/4[01;31m[K80[m[K39.py

Tourismscripts Hotel Portal - 'hotel_city' HTML Injection
| php/webapps/360[01;31m[K80[m[K.txt

TP-Link TD-W8951ND - Multiple Vulnerabilities
| hardware/webapps/2[01;31m[K80[m[K55.txt
```

TP-Link WR740N/WR740ND - Multiple Cross-Site Request Forgery Vulnerabilities |
hardware/webapps/29[01;31m[K80[m[K2.txt

TPTEST 3.1.7 - Stack Buffer Overflow (PoC)
| windows/dos/[01;31m[K80[m[K58.pl

Traidnt UP 1.0 - Arbitrary File Upload
| php/webapps/[01;31m[K80[m[K06.txt

Travel Portal Script - Cross-Site Request Forgery (Admin Password Change) |
php/webapps/152[01;31m[K80[m[K.html

Trend Micro - 'CoreServiceShell.exe' Multiple HTTP s
| windows/webapps/39[01;31m[K80[m[K8.txt

Trend Micro Deep Discovery 3.7/3.8 SP1 (3.81)/3.8 SP2 (3.82) - 'hotfix_upload.cgi' Filename Remote Code Ex |
linux/webapps/401[01;31m[K80[m[K.txt

Trend Micro OfficeScan Corporate Edition 3.0/3.5/3.11/3.13 - Denial of Service |
multiple/dos/197[01;31m[K80[m[K.txt

Trendnet Camera (Multiple Products) - Remote Security Bypass
| hardware/remote/366[01;31m[K80[m[K.txt

Tri-PLC Nano-10 r81 - Denial of Service
| hardware/dos/26[01;31m[K80[m[K2.py

Trillian 0.6351/0.7x - Identd Buffer Overflow
| windows/remote/21[01;31m[K80[m[K4.c

TSplus 16.0.0.0 - Remote Work Insecure Files and Folders
| windows/remote/516[01;31m[K80[m[K.txt

TufinOS 2.17 Build 1193 - XML External Entity Injection
| linux/webapps/45[01;31m[K80[m[K8.txt

Turnkey eBook Store 1.1 - 'keywords' Cross-Site Scripting
| php/webapps/328[01;31m[K80[m[K.txt

Twitter for iPhone - Man in the Middle Security
| ios/remote/3[01;31m[K80[m[K58.py

TYPO3 < 4.0.12/4.1.10/4.2.6 - 'jumpUrl' Remote File Disclosure
| php/webapps/[01;31m[K80[m[K38.py

TYPO3 CMS 4.0 - 'showUid' SQL Injection
| php/webapps/93[01;31m[K80[m[K.txt

Typo3 Extension JobControl 2.14.0 - Cross-Site Scripting / SQL Injection | php/webapps/34[01;31m[K80[m[K0.txt

U.S. Robotics USR[01;31m[K80[m[K[01;31m[K80[m[K54 Wireless Access Point - Web Administration Denial of Service | hardware/dos/24344.txt

UBBCentral UBB.Threads 6.0 - Remote File Inclusion | php/webapps/10[01;31m[K80[m[K3.txt

Ubisoft Rayman Legends 1.2.103716 - Remote Stack Buffer Overflow (PoC) | windows/dos/33[01;31m[K80[m[K4.pl

Uiga Personal Portal - Multiple Vulnerabilities | php/webapps/1[01;31m[K80[m[K02.txt

UNAK-CMS 1.5 - 'dirroot' Remote File Inclusion | php/webapps/23[01;31m[K80[m[K.txt

UnrealIRCd 3.2.8.1 - Local Configuration Stack Overflow | windows/dos/1[01;31m[K80[m[K11.txt

Uplay 92.0.0.62[01;31m[K80[m[K - Local Privilege Escalation | windows/local/47493.txt

User Registration & Login and User Management System 2.1 - Cross Site Request Forgery | php/webapps/491[01;31m[K80[m[K.txt

usersctp - Out-of-Bounds Reads in sctp_load_addresses_from_init | linux/dos/4[01;31m[K80[m[K34.py

UUSee 2008 - UUUpgrade ActiveX Control 'Update' Method Arbitrary File Download | windows/remote/319[01;31m[K80[m[K.html

V3 Chat Instant Messenger - '/mail/index.php?id' Cross-Site Scripting | php/webapps/2[01;31m[K80[m[K68.txt

V3 Chat Instant Messenger - '/mail/reply.php?id' Cross-Site Scripting | php/webapps/2[01;31m[K80[m[K69.txt

V3 Chat Instant Messenger - 'expire.php?cust_name' Cross-Site Scripting | php/webapps/2[01;31m[K80[m[K74.txt

V3 Chat Instant Messenger - 'mycontacts.php' membername Arbitrary User Buddy List Manipulation | php/webapps/2[01;31m[K80[m[K75.txt

V3 Chat Instant Messenger - 'online.php?site_id' Cross-Site Scripting | php/webapps/2[01;31m[K80[m[K70.txt

```
V3 Chat Instant Messenger - 'profile.php?site_id' Cross-Site Scripting
| php/webapps/2[01;31m[K80[m[K72.txt

V3 Chat Instant Messenger - 'profileview.php?membername' Cross-Site
Scripting                                |
php/webapps/2[01;31m[K80[m[K73.txt

V3 Chat Instant Messenger - 'search.php' Multiple Cross-Site Scripting
Vulnerabilities                     |
php/webapps/2[01;31m[K80[m[K71.txt

Vanilla Forums 2.0.18.4 - Tagging Persistent Cross-Site Scripting
| php/webapps/189[01;31m[K80[m[K.txt

Vanilla Forums 2.6.3 - Persistent Cross-Site Scripting
| php/webapps/4[01;31m[K80[m[K42.txt

Vastal I-Tech Mag Zone - 'cat_id' SQL Injection
| php/webapps/63[01;31m[K80[m[K.txt

VBTube 1.1 - Search Cross-Site Scripting
| php/webapps/30[01;31m[K80[m[K4.txt

vBulletin 1.0.1 lite/2.x/3.0 - '/admincp/user.php?email' Cross-Site
Scripting                                |
php/webapps/262[01;31m[K80[m[K.txt

vBulletin 2.x/3.x - Multiple Cross-Site Scripting Vulnerabilities
| php/webapps/2[01;31m[K80[m[K28.txt

vBulletin 3.0.9/3.5.x - 'member.php' Cross-Site Scripting
| php/webapps/2[01;31m[K80[m[K76.txt

vBulletin 3.5.1 - 'Vbugs.php' Cross-Site Scripting
| php/webapps/275[01;31m[K80[m[K.txt

vBulletin 4.1.12 - 'blog_plugin_useradmin.php' SQL Injection
| php/webapps/37[01;31m[K80[m[K7.txt

vBulletin < 3.0.0 RC4 - Cross Site Scripting
| php/webapps/43[01;31m[K80[m[K3.txt

VBZoom 1.0/1.1 - Multiple SQL Injections
| php/webapps/2[01;31m[K80[m[K18.txt

VBZoom 1.11 - 'forum.php' SQL Injection
| php/webapps/2[01;31m[K80[m[K33.txt

VCalendar - Remote Database Disclosure
| php/webapps/71[01;31m[K80[m[K.txt

VehicleWorkshop 1.0 - 'bookingid' SQL Injection
| php/webapps/4[01;31m[K80[m[K23.txt
```

VelotiSmart WiFi B-3[01;31m[K80[m[K Camera - Directory Traversal
| hardware/webapps/45030.txt

Veno File Manager - 'q' Arbitrary File Download
| php/webapps/388[01;31m[K80[m[K.txt

VeriCentre - Multiple SQL Injections
| php/webapps/3[01;31m[K80[m[K10.txt

Verodin Director Web Console 3.5.4.0 - Remote Authenticated Password Disclosure (PoC) |
json/webapps/4[01;31m[K80[m[K02.py

VeryPDF HTML Converter 2.0 - Local Buffer Overflow (SEH/ToLower() Bypass) |
windows/local/3[01;31m[K80[m[K95.pl

Viber 4.2.0 - Non-Printable Characters Handling Denial of Service
| ios/dos/3[01;31m[K80[m[K32.pl

VideoCharge Express 3.16.3.04 - Local Buffer Overflow
| windows/local/369[01;31m[K80[m[K.py

VIM 8.2 - Denial of Service (PoC)
| linux/dos/4[01;31m[K80[m[K08.txt

Virtual Freer 1.58 - Remote Command Execution
| php/webapps/4[01;31m[K80[m[K94.py

Visale 1.0 - 'pblscg.cgi?catsubno' Cross-Site Scripting
| cgi/webapps/276[01;31m[K80[m[K.txt

Vlinks 1.1.6 - 'id' SQL Injection
| php/webapps/[01;31m[K80[m[K50.txt

VMware Player 1.0.1 Build 19317 - '.VMX' File Denial of Service
| multiple/dos/2[01;31m[K80[m[K65.vmx

VMware Tools 3.1 - 'HGFS.Sys' Local Privilege Escalation
| windows/local/30[01;31m[K80[m[K2.c

VMware Virtual [01;31m[K80[m[K86 - Linux Local Ring0
| multiple/local/10207.txt

VocalTec VGW120/VGW4[01;31m[K80[m[K Telephony Gateway Remote H.225 - Denial of Service |
hardware/dos/24143.c

Vote-Pro 4.0 - 'poll_frame.php?poll_id' Remote Code Execution
| php/webapps/31[01;31m[K80[m[K.pl

VSAXESS V2.6.2.70 build20171226_053 - 'organization' Denial of Service (PoC) | windows/dos/45[01;31m[K80[m[K0.py

```
VTENEXT 19 CE - Remote Code Execution
| multiple/webapps/48[01;31m[K80[m[K4.py

vTiger CRM 5.0.4 - Local File Inclusion
| php/webapps/162[01;31m[K80[m[K.py

VuBB Forum RC1 - 'm' SQL Injection
| php/webapps/12[01;31m[K80[m[K.pl

w3bcms 3.5.0 - Multiple Vulnerabilities
| php/webapps/[01;31m[K80[m[K09.pl

War Times - Remote Game Server Denial of Service
| windows/dos/256[01;31m[K80[m[K.txt

WB News 2.1.1 - config[installdir] Remote File Inclusion
| php/webapps/[01;31m[K80[m[K26.txt

Web File Browser 0.4b14 - File Download
| php/webapps/1[01;31m[K80[m[K70.txt

Web Help Desk by SolarWinds - Persistent Cross-Site Scripting
| php/webapps/21[01;31m[K80[m[K9.txt

WebcamXP 3.72.440/4.05.2[01;31m[K80[m[K Beta - '/pocketpc?camnum'
Arbitrary Memory Disclosure                          |
multiple/webapps/31233.txt

WebcamXP 3.72.440/4.05.2[01;31m[K80[m[K Beta - '/show_gallery_pic?id'
Arbitrary Memory Disclosure                      |
multiple/webapps/31234.txt

WebChamado 1.1 - 'tsk_id' SQL Injection
| php/webapps/5[01;31m[K80[m[K2.txt

webConductor - 'default.asp' SQL Injection
| asp/webapps/341[01;31m[K80[m[K.txt

webframe 0.76 - Multiple File Inclusions
| php/webapps/[01;31m[K80[m[K25.txt

webid 1.0.4 - Multiple Vulnerabilities
| php/webapps/205[01;31m[K80[m[K.txt

WEBIGniter v28.7.23 - Stored Cross Site Scripting (XSS)
| php/webapps/51[01;31m[K80[m[K7.txt

WebKit - 'WebCore::SVGAnimateElementBase::resetAnimatedType' Use-After-
Free                                  |
multiple/dos/454[01;31m[K80[m[K.html
```

WebKit Cross-Site Scripting Filter - 'Cross-Site ScriptingAuditor.cpp' Security Bypass |
php/webapps/3[01;31m[K80[m[K24.txt

Webmin 1.5[01;31m[K80[m[K - '/file/show.cgi' Remote Command Execution (Metasploit) |
unix/remote/21851.rb

Webmin 1.984 - Remote Code Execution (Authenticated)
| linux/webapps/50[01;31m[K80[m[K9.py

Websense Email Security - Denial of Service
| hardware/dos/99[01;31m[K80[m[K.txt

Webster HTTP Server - GET Buffer Overflow (Metasploit)
| windows/remote/16[01;31m[K80[m[K2.rb

WebWasher Classic 2.2/3.3 - Error Message Cross-Site Scripting
| multiple/remote/233[01;31m[K80[m[K.txt

Wedding Slideshow Studio 1.36 - 'Key' Buffer Overflow
| windows/local/4[01;31m[K80[m[K28.py

Wedding Slideshow Studio 1.36 - 'Name' Buffer Overflow
| windows/local/4[01;31m[K80[m[K50.py

WePresent WiPG-1500 - Backdoor Account
| hardware/remote/414[01;31m[K80[m[K.txt

WHMCompleteSolution (WHMCS) 3.x - 'clientarea.php' Local File Disclosure |
php/webapps/1[01;31m[K80[m[K81.txt

WHMCompleteSolution (WHMCS) 5.2.7 - SQL Injection
| php/webapps/28[01;31m[K80[m[K7.py

WHMCompleteSolution 3.x/4.x - Multiple Vulnerabilities
| php/webapps/1[01;31m[K80[m[K88.txt

Wikidforum 2.20 - Cross-Site Scripting
| php/webapps/455[01;31m[K80[m[K.txt

Winamp - '.flv' File Processing Memory Corruption
| windows/dos/391[01;31m[K80[m[K.pl

Windscribe - WindscribeService Named Pipe Privilege Escalation (Metasploit) |
windows/local/4[01;31m[K80[m[K21.rb

WinRAR 5.[01;31m[K80[m[K (x64) - Denial of Service
| windows_x86-64/dos/47525.txt

```
Winrar 5.[01;31m[K80[m[K - XML External Entity Injection
| xml/local/47526.txt

WinSCP 3.8.1 - URI Handler Arbitrary File Access
| windows/remote/2[01;31m[K80[m[K07.txt

Wolf CMS - Arbitrary File Upload / Execution
| php/webapps/3[01;31m[K80[m[K00.txt

Woltlab Burning Board 1.2/2.0/2.3 - 'newthread.php?boardid' SQL
Injection                                    |
php/webapps/2[01;31m[K80[m[K89.txt

Woltlab Burning Board 1.2/2.0/2.3 - 'report.php?postid' SQL Injection
| php/webapps/2[01;31m[K80[m[K90.txt

Woltlab Burning Board 1.2/2.0/2.3 - 'showmods.php?boardid' SQL
Injection                                     |
php/webapps/2[01;31m[K80[m[K91.txt

Woltlab Burning Board 2.x - Multiple SQL Injections
| php/webapps/2[01;31m[K80[m[K22.txt

Wondercms 4.3.2 - XSS to RCE
| multiple/webapps/51[01;31m[K80[m[K5.py

WordPress Core 2.0.5 - 'functions.php' Remote File Inclusion
| php/webapps/289[01;31m[K80[m[K.txt

WordPress Core < 5.3.x - 'xmlrpc.php' Denial of Service
| php/dos/47[01;31m[K80[m[K0.py

WordPress Plugin 1 Flash Gallery 1.30 < 1.5.7a - Arbitrary File Upload
(Metasploit)                         | php/webapps/17[01;31m[K80[m[K1.rb

WordPress Plugin A to Z Category Listing 1.3 - SQL Injection
| php/webapps/17[01;31m[K80[m[K9.txt

WordPress Plugin Accept Signups 0.1 - Cross-Site Scripting
| php/webapps/15[01;31m[K80[m[K8.txt

WordPress Plugin Ads Box - 'count' SQL Injection
| php/webapps/3[01;31m[K80[m[K60.txt

WordPress Plugin Ads Pro < 3.4 - Cross-Site Scripting / SQL Injection
| php/webapps/423[01;31m[K80[m[K.txt

Wordpress Plugin Catch Themes Demo Import 1.6.1 - Remote Code Execution
(RCE) (Authenticated)              | php/webapps/505[01;31m[K80[m[K.py

WordPress Plugin church_admin 0.[01;31m[K80[m[K0 - Persistent Cross-
Site Scripting                                        |
php/webapps/37112.txt
```

```
WordPress Plugin Community Events 1.3.5 - SQL Injection
| php/webapps/36[01;31m[K80[m[K5.txt

WordPress Plugin Contact Form 2.7.5 - SQL Injection
| php/webapps/179[01;31m[K80[m[K.txt

WordPress Plugin Contact Form Generator 2.0.1 - Multiple Cross-Site
Request Forgery Vulnerabilities        |
php/webapps/3[01;31m[K80[m[K86.html

WordPress Plugin contact-form-7 5.1.6 - Remote File Upload
| php/webapps/4[01;31m[K80[m[K62.txt

WordPress Plugin Easy Contact Form Lite 1.0.7 - SQL Injection
| php/webapps/176[01;31m[K80[m[K.txt

WordPress Plugin Eco-annu - 'eid' SQL Injection
| php/webapps/3[01;31m[K80[m[K19.txt

WordPress Plugin FLV Player - 'id' SQL Injection
| php/webapps/3[01;31m[K80[m[K12.txt

WordPress Plugin Glossary - SQL Injection
| php/webapps/1[01;31m[K80[m[K55.txt

WordPress Plugin HDW Player - '/wp-admin/admin.php' SQL Injection
| php/webapps/392[01;31m[K80[m[K.txt

WordPress Plugin Hospital Management System - SQL Injection
| php/webapps/42[01;31m[K80[m[K2.txt

WordPress Plugin Huge-IT Image Gallery 1.8.9 - Multiple Vulnerabilities
| php/webapps/39[01;31m[K80[m[K7.txt

WordPress Plugin IndiaNIC Testimonial - Multiple Vulnerabilities
| php/webapps/2[01;31m[K80[m[K54.txt

WordPress Plugin InfiniteWP - Client Authentication Bypass (Metasploit)
| php/webapps/4[01;31m[K80[m[K47.rb

WordPress Plugin LearnDash LMS 3.1.2 - Reflective Cross-Site Scripting
| php/webapps/4[01;31m[K80[m[K30.txt

WordPress Plugin Media File Manager 1.4.2 - Directory Traversal /
Cross-Site Scripting                    |
php/webapps/45[01;31m[K80[m[K9.txt

WordPress Plugin MiwoFTP 1.0.5 - Arbitrary File Download (2)
| php/webapps/36[01;31m[K80[m[K1.txt

WordPress Plugin NewsLetter Manager 1.0 - Multiple Cross-Site Scripting
Vulnerabilities                   | php/webapps/371[01;31m[K80[m[K.txt
```

```
WordPress Plugin NEX-Forms < 3.0 - SQL Injection
| php/webapps/36[01;31m[K80[m[K0.txt

WordPress Plugin Ninja Forms 3.3.17 - Cross-Site Scripting
| php/webapps/458[01;31m[K80[m[K.txt

WordPress Plugin Olimometer 2.56 - SQL Injection
| php/webapps/40[01;31m[K80[m[K4.txt

WordPress Plugin PHP Event Calendar - 'cid' SQL Injection
| php/webapps/3[01;31m[K80[m[K18.txt

WordPress Plugin Plg Novana - 'id' SQL Injection
| php/webapps/3[01;31m[K80[m[K48.txt

WordPress Plugin Q and A (Focus Plus) FAQ 1.3.9.7 - Multiple
Vulnerabilities                                  |
php/webapps/39[01;31m[K80[m[K6.txt

WordPress Plugin Quick Contact Form 6.0 - Persistent Cross-Site
Scripting                                       |
php/webapps/28[01;31m[K80[m[K8.txt

WordPress Plugin Reflex Gallery - Arbitrary File Upload (Metasploit)
| php/remote/36[01;31m[K80[m[K9.rb

WordPress Plugin School Management System - SQL Injection
| php/webapps/42[01;31m[K80[m[K4.txt

WordPress Plugin Share and Follow 1.[01;31m[K80[m[K.3 - 'admin.php'
Cross-Site Scripting                                    |
php/webapps/37202.txt

WordPress Plugin Spicy Blogroll - Local File Inclusion
| php/webapps/26[01;31m[K80[m[K4.txt

WordPress Plugin Stop Spammers 2021.8 - 'log' Reflected Cross-site
Scripting (XSS)                             |
php/webapps/498[01;31m[K80[m[K.txt

WordPress Plugin Strong Testimonials 2.40.1 - Persistent Cross-Site
Scripting                                   |
php/webapps/4[01;31m[K80[m[K76.txt

WordPress Plugin Tagged Albums - 'id' SQL Injection
| php/webapps/3[01;31m[K80[m[K23.txt

WordPress Plugin Tune Library 1.5.4 - SQL Injection
| php/webapps/36[01;31m[K80[m[K2.txt

WordPress Plugin Tutor.1.5.3 - Local File Inclusion
| php/webapps/4[01;31m[K80[m[K58.txt
```

WordPress Plugin tutor.1.5.3 - Persistent Cross-Site Scripting
| php/webapps/4[01;31m[K80[m[K59.txt

WordPress Plugin ultimate-member 2.1.3 - Local File Inclusion
| php/webapps/4[01;31m[K80[m[K65.txt

WordPress Plugin Video Lead Form - 'errMsg' Cross-Site Scripting
| php/webapps/3[01;31m[K80[m[K66.txt

WordPress Plugin Visual Slide Box Builder 3.2.9 - SQLi
| php/webapps/509[01;31m[K80[m[K.txt

WordPress Plugin Webplayer - 'id' SQL Injection
| php/webapps/3[01;31m[K80[m[K47.txt

WordPress Plugin WOOF Products Filter for WooCommerce 1.2.3 -
Persistent Cross-Site Scripting |
php/webapps/4[01;31m[K80[m[K88.txt

WordPress Plugin Wordfence.7.4.5 - Local File Disclosure
| php/webapps/4[01;31m[K80[m[K61.txt

WordPress Plugin WP Private Messages 1.0.1 - SQL Injection (2)
| php/webapps/411[01;31m[K80[m[K.txt

WordPress Plugin WP Sitemap Page 1.6.2 - Persistent Cross-Site
Scripting |
php/webapps/4[01;31m[K80[m[K93.txt

WordPress Plugin WP Symposium 15.1 - '&show=' SQL Injection
| php/webapps/370[01;31m[K80[m[K.txt

WordPress Plugin WP-Client 3.8.7 - Persistent Cross-Site Scripting
| php/webapps/38[01;31m[K80[m[K3.txt

WordPress Plugin WP-Filebase Download Manager 0.2.9 - SQL Injection
| php/webapps/17[01;31m[K80[m[K8.txt

WordPress Plugin WP-Realty - 'listing_id' SQL Injection
| php/webapps/38[01;31m[K80[m[K8.txt

WordPress Plugin WPAMS - SQL Injection
| php/webapps/42[01;31m[K80[m[K5.txt

WordPress Plugin WPCHURCH - SQL Injection
| php/webapps/42[01;31m[K80[m[K0.txt

WordPress Plugin WPGraphQL 1.3.5 - Denial of Service
| php/dos/49[01;31m[K80[m[K7.py

WordPress Plugin WPGYM - SQL Injection
| php/webapps/42[01;31m[K80[m[K1.txt

WordPress Plugin wptouch - SQL Injection
| php/webapps/1[01;31m[K80[m[K39.txt

WordPress Plugin Zarzadzonie Kontem - 'ajaxfilemanager.php' Script
Arbitrary File Upload |
php/webapps/3[01;31m[K80[m[K50.txt

WordPress Plugin Zingiri Web Shop - 'path' Arbitrary File Upload
| php/webapps/3[01;31m[K80[m[K46.txt

WordPress Plugin Zingiri Web Shop 2.4.2 - Persistent Cross-Site
Scripting |
php/webapps/18[01;31m[K80[m[K6.txt

WordPress Theme classipress 3.1.4 - Persistent Cross-Site Scripting
| php/webapps/1[01;31m[K80[m[K53.txt

WordPress Theme CStar Design - 'id' SQL Injection
| php/webapps/3[01;31m[K80[m[K64.txt

WordPress Theme Dailyedition-mouss - 'id' SQL Injection
| php/webapps/3[01;31m[K80[m[K22.txt

WordPress Theme F8 Lite 4.2.1 - 's' Cross-Site Scripting
| php/webapps/361[01;31m[K80[m[K.txt

WordPress Theme Fruitful 3.8 - Persistent Cross-Site Scripting
| php/webapps/4[01;31m[K80[m[K83.txt

WordPress Theme Kakao - 'ID' SQL Injection
| php/webapps/3[01;31m[K80[m[K17.txt

WordPress Theme Madebymilk - 'id' SQL Injection
| php/webapps/3[01;31m[K80[m[K41.txt

WordPress Theme Magazine Basic - 'id' SQL Injection
| php/webapps/3[01;31m[K80[m[K57.txt

WordPress Theme Toolbox - 'mls' SQL Injection
| php/webapps/3[01;31m[K80[m[K77.txt

WordPress Theme Wp-ImageZoom - 'id' SQL Injection
| php/webapps/3[01;31m[K80[m[K63.txt

WSN Knowledge Base 1.2 - 'comments.php?id' SQL Injection
| php/webapps/266[01;31m[K80[m[K.txt

wwwThreads - 'calendar.php' Cross-Site Scripting
| php/webapps/282[01;31m[K80[m[K.txt

WyMIEN PHP 1.0 - 'index.php' Cross-Site Scripting
| php/webapps/318[01;31m[K80[m[K.txt

X.Org xorg 1.4 < 1.11.2 - File Permission Change
| linux/local/1[01;31m[K80[m[K40.c

X10media Mp3 Search Engine 1.5.5 - Remote File Inclusion
| php/webapps/64[01;31m[K80[m[K.txt

XAMPP - Buffer Overflow POC
| windows/dos/51[01;31m[K80[m[K0.py

XCMS 1.82 - Local/Remote File Inclusion
| php/webapps/4[01;31m[K80[m[K2.txt

Xcode OpenBase 9.1.5 (OSX) - Root File Create Privilege Escalation
| osx/local/25[01;31m[K80[m[K.pl

Xerox 4595 - Denial of Service
| hardware/dos/153[01;31m[K80[m[K.py

Xerox AltaLink C[01;31m[K80[m[K35 Printer - Cross-Site Request Forgery
(Add Admin) |
hardware/webapps/47787.txt

XGI Windows VGA Display Manager 6.14.10.1090 - Arbitrary Write (PoC)
| windows/dos/3[01;31m[K80[m[K55.txt

xglance-bin 11.00 - Privilege Escalation
| linux/local/4[01;31m[K80[m[K00.sh

Xilisoft Video Converter 3.1.8.0720b - '.ogg' Buffer Overflow
| windows/dos/344[01;31m[K80[m[K.py

XiVO - Cross-Site Request Forgery
| php/webapps/3[01;31m[K80[m[K45.html

XM Easy Personal FTP Server 5.8.0 - Denial of Service (Metasploit)
| windows/dos/9[01;31m[K80[m[K4.rb

xml2owl 0.1.1 - 'showcode.php' Remote Command Execution
| php/webapps/4[01;31m[K80[m[K0.txt

xmonad XMonad.Hooks.DynamicLog Module - Multiple Remote Command
Injection Vulnerabilities |
linux/remote/386[01;31m[K80[m[K.html

XnConvert 1.82 - Denial of Service (PoC)
| windows/dos/47[01;31m[K80[m[K1.py

Xoops 1.3.5 - Private Message System Font Attributes HTML Injection
| php/webapps/220[01;31m[K80[m[K.txt

Xoops 2.2.3 - 'search.php' Cross-Site Scripting
| php/webapps/28[01;31m[K80[m[K3.txt

```
XOOPS 2.3.1 - Multiple Local File Inclusions
| php/webapps/73[01;31m[K80[m[K.txt

XOOPS Module dictionary 2.0.18 - 'detail.php' SQL Injection
| php/webapps/10[01;31m[K80[m[K7.txt

Xpand Rally 1.0.0.0 (Server/Clients) - Crash
| windows/dos/7[01;31m[K80[m[K.c

YACS CMS 8.11 - 'update_trailer.php' Remote File Inclusion
| php/webapps/[01;31m[K80[m[K66.txt

Yahoo! Messenger 7.0/7.5 - 'jscript.dll' Non-ASCII Character Denial of
Service                              |
windows/dos/2[01;31m[K80[m[K99.txt

Yanf 0.4 - HTTP Response Buffer Overflow
| multiple/remote/249[01;31m[K80[m[K.txt

Yaws < 1.[01;31m[K80[m[K - Multiple Headers Remote Denial of Service
Vulnerabilities                                    |
multiple/dos/8148.pl

YeSiL KoRiDoR Ziyaretçi Defteri - 'index.php' SQL Injection
| php/webapps/310[01;31m[K80[m[K.txt

YesWiki 0.2 - 'squelette' Directory Traversal
| php/webapps/3[01;31m[K80[m[K71.rb

Yet Another NOCC 0.1.0 - Local File Inclusion
| php/webapps/[01;31m[K80[m[K20.txt

Yosoro 1.0.4 - Remote Code Execution
| macos/webapps/44[01;31m[K80[m[K3.txt

YourFreeWorld Ad-Exchange Script - 'id' SQL Injection
| php/webapps/322[01;31m[K80[m[K.txt

Zapya Desktop 1.[01;31m[K80[m[K3 - 'ZapyaService.exe' Local Privilege
Escalation                                         |
windows/local/40365.txt

ZeeCareers 2.0 - 'addAdminmembercode.php' Arbitrary Add Admin
| php/webapps/8[01;31m[K80[m[K9.html

zeeproperty - 'adid' SQL Injection
| php/webapps/67[01;31m[K80[m[K.txt

Zeeways Script - Multiple Vulnerabilities
| php/webapps/12[01;31m[K80[m[K5.txt

ZenPhoto 1.4.1.4 - 'ajax_create_folder.php' Remote Code Execution
| php/webapps/1[01;31m[K80[m[K83.php
```

Zeroboard4 pl8 (07.12.17) - Multiple Vulnerabilities
| php/webapps/[01;31m[K80[m[K00.txt

ZeroBoardXE 1.1.5 (09.01.22) - Cross-Site Scripting
| php/webapps/[01;31m[K80[m[K19.txt

ZeroShell 1.0beta11 - Remote Code Execution
| hardware/remote/[01;31m[K80[m[K23.txt

zFeeder 1.6 - 'admin.php' Admin Bypass
| php/webapps/[01;31m[K80[m[K92.txt

zFTPServer - 'cwd/stat' Remote Denial of Service
| windows/dos/1[01;31m[K80[m[K28.py

Zhone ADSL2+ 4P Bridge & Router (Broadcom) - Multiple Vulnerabilities
| hardware/webapps/3[01;31m[K80[m[K[01;31m[K80[m[K.txt

Zix Forum 1.12 - 'layid' SQL Injection
| asp/webapps/1[01;31m[K80[m[K7.txt

Zoo Management System 1.0 - Authentication Bypass
| php/webapps/488[01;31m[K80[m[K.txt

Zoom Telephonics ADSL Modem/Router - Multiple Vulnerabilities
| hardware/webapps/2[01;31m[K80[m[K53.txt

ZTE Router F602W - Captcha Bypass
| hardware/webapps/48[01;31m[K80[m[K1.sh

ZTE WXV10 W300 - Multiple Vulnerabilities
| hardware/webapps/33[01;31m[K80[m[K3.txt

ZTE ZXDSL 831IIV7.5.0a_Z29_OV - Multiple Vulnerabilities
| hardware/webapps/1[01;31m[K80[m[K61.txt

ZTE ZXDSL-931VII - Configuration Dump
| hardware/webapps/346[01;31m[K80[m[K.txt

Zyxel Armor X1 WAP6[01;31m[K80[m[K6 - Directory Traversal
| hardware/webapps/48669.txt

Shellcode Title
| Path

Alpha - /bin/sh Shellcode ([01;31m[K80[m[K bytes)
| alpha/434[01;31m[K80[m[K.c

FreeBSD/x64 - execve(/bin/sh) Shellcode (34 bytes)
| freebsd_x86-64/132[01;31m[K80[m[K.c

FreeBSD/x86 - Reverse (127.0.0.1:[01;31m[K80[m[K00/TCP) Shell (/bin/sh)
+ Null-Free Shellcode (89 bytes) | freebsd_x86/13267.asm

FreeBSD/x86 - Reverse (192.168.1.33:[01;31m[K80[m[K00/TCP) cat
/etc/passwd Shellcode (112 bytes) |
freebsd_x86/13263.txt

FreeBSD/x86 - Reverse Connection (172.17.0.9:[01;31m[K80[m[K00/TCP) +
Receive Shellcode + Payload Loader + Return Resul | freebsd_x86/13265.c

Linux/ARM - Reverse (192.168.1.1:4444/TCP) Shell (/bin/sh)+ Null-Free
Shellcode ([01;31m[K80[m[K bytes) | arm/43921.asm

Linux/MIPS (Little Endian) - system(telnetd -l /bin/sh) Shellcode
([01;31m[K80[m[K bytes) |
linux_mips/27132.txt

Linux/x64 - execve(/bin/sh -c reboot) Shellcode (89 bytes)
| linux_x86-64/40[01;31m[K80[m[K8.c

Linux/x64 - XANAX Decoder Shellcode (127 bytes)
| generator/466[01;31m[K80[m[K.nasm

Linux/x86 - Bind (1337/TCP) Ncat (/usr/bin/ncat) Shell (/bin/bash) +
Null-Free Shellcode (95 bytes) | linux_x86/459[01;31m[K80[m[K.c

Linux/x86 - Bind (31337/TCP) Shell (/bin/sh) Shellcode ([01;31m[K80[m[K
bytes) | linux_x86/13387.c

Linux/x86 - Bind (4444/TCP) Shell (/bin/sh) + IPv6 Shellcode (100
bytes) |
linux_x86/450[01;31m[K80[m[K.c

Linux/x86 - Bind (4444/TCP) Shell (/bin/sh) Shellcode (105 bytes)
| linux_x86/44[01;31m[K80[m[K8.c

Linux/x86 - Bind ([01;31m[K80[m[K00/TCP) Shell (/bin/sh) Shellcode (179
bytes) | linux_x86/13319.s

Linux/x86 - Bind ([01;31m[K80[m[K00/TCP) Shell + Add Root User
Shellcode (225+ bytes) |
linux_x86/13318.s

Linux/x86 - Bind ([01;31m[K80[m[K00/TCP) Shell + Flush IPTables Rules (/sbin/iptables -F) Shellcode (176 bytes) | linux_x86/13317.s

Linux/x86 - Bind ([01;31m[K80[m[K[01;31m[K80[m[K/TCP) Netcat (/bin/nc) Shell (/bin/sh) Shellcode (75 bytes) | linux_x86/14332.c

Linux/x86 - Bind Shell Generator Shellcode (114 bytes) | linux_x86/4[01;31m[K80[m[K32.py

Linux/x86 - Break chroot + execve(/bin/sh) Shellcode ([01;31m[K80[m[K bytes) | linux_x86/13454.c

Linux/x86 - cat .bash_history + base64 Encode + cURL (http://localhost:[01;31m[K80[m[K[01;31m[K80[m[K) Shellcode (125 bytes) | linux_x86/46704.txt

Linux/x86 - Create File With Permission 7775 + exit() Shellcode (Generator) | generator/3[01;31m[K80[m[K94.py

Linux/x86 - Disable ASLR Security Shellcode ([01;31m[K80[m[K bytes) | linux_x86/41969.c

Linux/x86 - Download File (HTTP/1.x http://127.0.0.1:[01;31m[K80[m[K81/foobar.bin) + Receive + Payload Loader Shellcode | linux_x86/133[01;31m[K80[m[K.c

Linux/x86 - Egghunter (0xdeadbeef) + access() + execve(/bin/sh) Shellcode (38 bytes) | linux_x86/44[01;31m[K80[m[K7.c

Linux/x86 - execve(/bin/bash) Shellcode (31 bytes) | linux_x86/3[01;31m[K80[m[K88.c

Linux/x86 - execve(/bin/sh -c) + wget (http://127.0.0.1:[01;31m[K80[m[K[01;31m[K80[m[K/evilfile) + chmod 777 + Execute Shellcode (11 | linux_x86/46103.c

Linux/x86 - execve(/bin/sh) Shellcode (20 bytes) | linux_x86/46[01;31m[K80[m[K9.c

Linux/x86 - Fork Bomb + Polymorphic Shellcode (30 bytes) | linux_x86/136[01;31m[K80[m[K.c

Linux/x86 - HTTP Server (8[01;31m[K80[m[K0/TCP) + fork() Shellcode (166 bytes) | linux_x86/13308.c

Linux/x86 - Multiple keys XOR Encoder / Decoder execve(/bin/sh) Shellcode (59 bytes) | generator/46[01;31m[K80[m[K0.txt

Linux/x86 - Reverse (/TCP) Netcat + mkfifo (-e option disabled) Shell (localhost:9999) Shellcode (1[01;31m[K80[m[K byte | linux_x86/40872.c

Linux/x86 - Reverse (127.0.0.1:[01;31m[K80[m[K/TCP) Shell + XOR Encoded Shellcode (371 bytes) | linux_x86/13366.txt

Linux/x86 - Reverse (127.0.0.1:[01;31m[K80[m[K[01;31m[K80[m[K/TCP) Shell (/bin/sh) Shellcode (91 Bytes) (Generator) | generator/46789.txt

Linux/x86 - Reverse (127.255.255.254:9090/TCP) Shell (/bin/zsh) Shellcode ([01;31m[K80[m[K bytes) | linux_x86/40223.c

Linux/x86 - Reverse ([01;31m[K80[m[K[01;31m[K80[m[K/TCP) Netcat Shell Shellcode (76 bytes) | linux_x86/14334.c

Linux/x86 - Reverse (localhost:[01;31m[K80[m[K[01;31m[K80[m[K/TCP) Shell + SSL Shellcode (422 bytes) | linux_x86/17371.c

Linux/x86 - Search For '.PHP'/'.HTML' Writable Files + Add Code Shellcode (3[01;31m[K80[m[K+ bytes) | linux_x86/18379.c

Linux/x86 - setuid(0) + execve(/bin/sh_ 0_ 0) Shellcode (27 bytes) | linux_x86/436[01;31m[K80[m[K.c

Linux/x86 - Shred File (test.txt) Shellcode (72 bytes) | linux_x86/46[01;31m[K80[m[K1.txt

Linux/x86 - Socket-Proxy (31337:11.22.33.44:[01;31m[K80[m[K) Shellcode (372 bytes) | linux_x86/13402.c

Linux/x86 - TCP Proxy (192.168.1.16:12[01;31m[K80[m[K/TCP) All Connect() + Null-Free Shellcode (236 bytes) | linux_x86/13381.c

Linux/x86 / Unix/SPARC - execve(/bin/sh) Shellcode ([01;31m[K80[m[K bytes) | multiple/13468.c

Mainframe/System Z - Bind (12345/TCP) Shell + Null-Free Shellcode (2488 bytes) | system_z/3[01;31m[K80[m[K75.txt

OSX/PPC - Add Root User (r00t) Shellcode (219 bytes) | osx_ppc/134[01;31m[K80[m[K.c

OSX/PPC - Bind ([01;31m[K80[m[K00/TCP) Shell + OSXPPCLongXOR Encoded Shellcode (300 bytes) | osx_ppc/43615.c

OSX/x64 - execve(/bin/sh) + Null-Free Shellcode (34 bytes) | osx/3[01;31m[K80[m[K65.txt

Solaris/MIPS - Download File (http://10.1.1.2:[01;31m[K80[m[K/evil-dl)
+ Execute (/tmp/ff) Shellcode (278 bytes) | solaris_mips/13489.c

Windows/ARM (RT) - Bind (4444/TCP) Shell Shellcode
| arm/271[01;31m[K80[m[K.asm

Windows/x86 (XP SP3) - Restart Shellcode (57 bytes)
| windows_x86/367[01;31m[K80[m[K.c

Windows/x86 - Download File
(http://10.10.10.5:[01;31m[K80[m[K[01;31m[K80[m[K/2NWyfQ9T.hta) Via
mshta + Execute + Stager Shellcode (| windows_x86/49466.asm

Windows/x86 - Download File
(http://192.168.43.192:[01;31m[K80[m[K[01;31m[K80[m[K/9MKWaRO.hta) Via
mshta Shellcode (100 bytes) | windows_x86/48718.c

Windows/x86 - Dynamic Bind Shell + Null-Free Shellcode (571 Bytes)
| windows_x86/479[01;31m[K80[m[K.txt

Port: 8009

Exploit Title
| Path

AWAuctionScript CMS - Multiple Remote Vulnerabilities
| php/webapps/3[01;31m[K8009[m[K.txt

Cisco AnyConnect 3.1.0[01;31m[K8009[m[K - Local Privilege Escalation
(via DMG Install Script) | osx/local/38303.c

Cisco AnyConnect Secure Mobility Client 3.1.0[01;31m[K8009[m[K - Local
Privilege Escalation |
windows/local/38289.txt

ELAN Smart-Pad 11.10.15.1 - 'ETDService' Unquoted Service Path
| windows/local/4[01;31m[K8009[m[K.txt

Five Star Review Script - 'index2.php?sort' Cross-Site Scripting
| php/webapps/2[01;31m[K8009[m[K.txt

Pre Studio Business Cards Designer - SQL Injection
| asp/webapps/1[01;31m[K8009[m[K.txt

w3bcms 3.5.0 - Multiple Vulnerabilities
| php/webapps/[01;31m[K8009[m[K.pl

Shellcodes: No Results