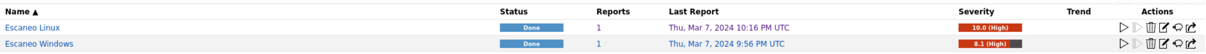
Práctica 2 INT

Identificación de vulnerabilidades

María Andrea Ugarte Valencia

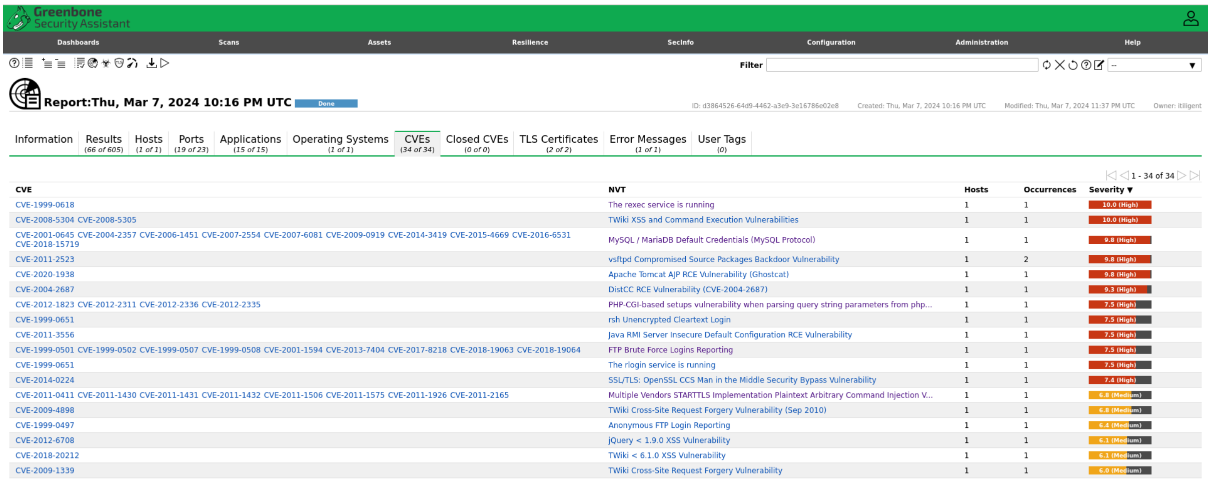
1 - Identificación de CVE

Realizamos un análisis completo de la máquina Windows y la máquina Linux con OPENVAS, una herramienta de escaneo de vulnerabilidades de código abierto. Una vez realizados los análisis, obtendremos los reportes:



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Escaneo Linux	Done	1	Thu, Mar 7, 2024 10:16 PM UTC	10.0 (High)		
Escaneo Windows	Done	1	Thu, Mar 7, 2024 9:56 PM UTC	8.1 (High)		

Los reportes generados por OpenVAS nos dan detalles sobre cada vulnerabilidad, como la prueba de red (NVT), un resumen del hallazgo y posibles soluciones para abordar la vulnerabilidad. También clasifican las vulnerabilidades según su gravedad:



Report:Thu, Mar 7, 2024 10:16 PM UTC Done

ID: d3864526-64d9-4462-a3e9-3e16786e02e8 Created: Thu, Mar 7, 2024 10:16 PM UTC Modified: Thu, Mar 7, 2024 11:37 PM UTC Owner: itiligent

Information | Results (66 of 605) | Hosts (1 of 1) | Ports (19 of 23) | Applications (15 of 15) | Operating Systems (1 of 1) | CVEs (34 of 34) | Closed CVEs (0 of 0) | TLS Certificates (2 of 2) | Error Messages (1 of 1) | User Tags (0)

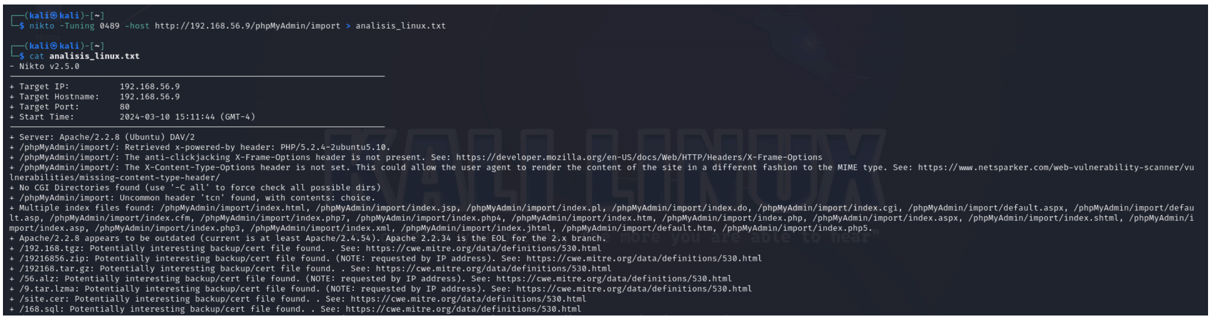
1 - 34 of 34

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-1999-0618	The rexec service is running	1	1	10.0 (High)
CVE-2008-5304 CVE-2008-5305	TWiki XSS and Command Execution Vulnerabilities	1	1	10.0 (High)
CVE-2001-0645 CVE-2004-2357 CVE-2006-1451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-3419 CVE-2015-4669 CVE-2016-6531 CVE-2018-15719	MySQL / MariaDB Default Credentials (MySQL Protocol)	1	1	9.8 (High)
CVE-2011-2523	vsftpd Compromised Source Packages Backdoor Vulnerability	1	2	9.8 (High)
CVE-2020-1938	Apache Tomcat AJP RCE Vulnerability (Ghostcat)	1	1	9.8 (High)
CVE-2004-2687	DistCC RCE Vulnerability (CVE-2004-2687)	1	1	9.3 (High)
CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335	PHP-CGI-based setups vulnerability when parsing query string parameters from php...	1	1	7.5 (High)
CVE-1999-0651	rsh Unencrypted Cleartext Login	1	1	7.5 (High)
CVE-2011-3556	Java RMI Server Insecure Default Configuration RCE Vulnerability	1	1	7.5 (High)
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2001-1594 CVE-2013-7404 CVE-2017-8218 CVE-2018-19063 CVE-2018-19064	FTP Brute Force Logins Reporting	1	1	7.5 (High)
CVE-1999-0651	The rlogin service is running	1	1	7.5 (High)
CVE-2014-0224	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	1	1	7.4 (High)
CVE-2011-0411 CVE-2011-1430 CVE-2011-1431 CVE-2011-1432 CVE-2011-1506 CVE-2011-1575 CVE-2011-1926 CVE-2011-2165	Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection V...	1	1	6.8 (Medium)
CVE-2009-4898	TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)	1	1	6.8 (Medium)
CVE-1999-0497	Anonymous FTP Login Reporting	1	1	6.4 (Medium)
CVE-2012-6708	jQuery < 1.9.0 XSS Vulnerability	1	1	6.1 (Medium)
CVE-2018-20212	TWiki < 6.1.0 XSS Vulnerability	1	1	6.1 (Medium)
CVE-2009-1339	TWiki Cross-Site Request Forgery Vulnerability	1	1	6.0 (Medium)

Además, vamos a utilizar la herramienta Nikto, un escáner de vulnerabilidades de código abierto especializado en servidores web, para llevar a cabo un análisis en la máquina Linux. Para personalizar nuestro escaneo, aprovecharemos la opción -Tuning, que nos permite especificar las pruebas a realizar.

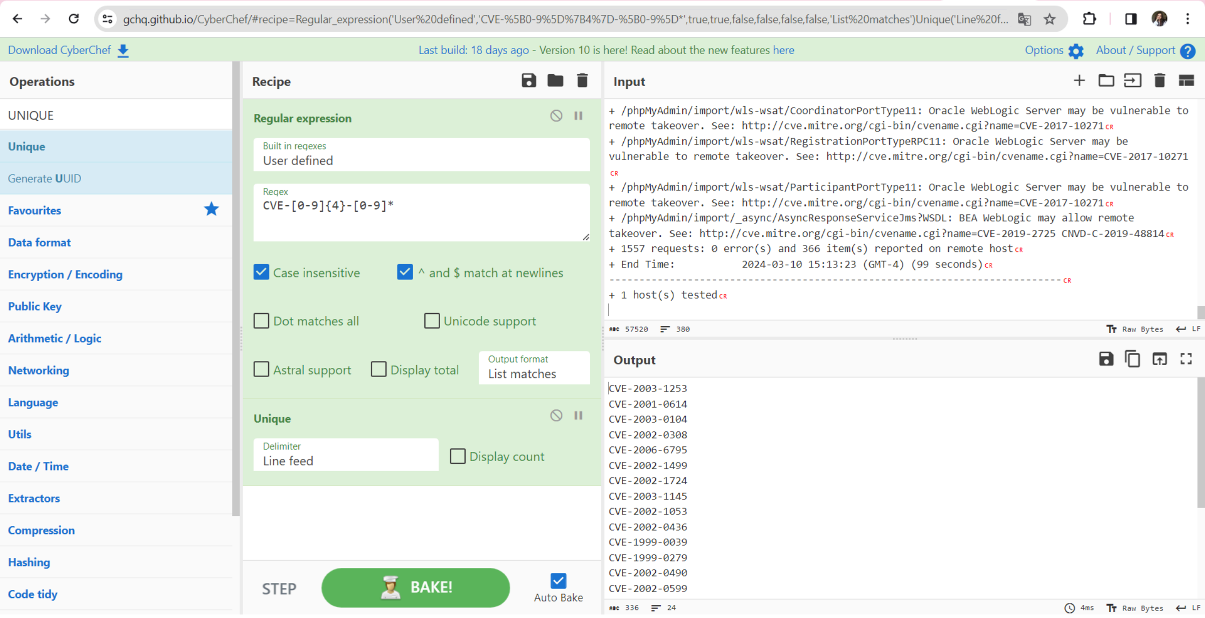
Debido a que llevar a cabo un escaneo directorio a directorio puede llevar mucho tiempo y no siempre proporciona información significativa, optamos por enfocar el análisis en un único directorio, en este caso, /phpMyAdmin/import. Este directorio es relevante y puede contener vulnerabilidades comunes. Hemos seleccionado las opciones 0 (Subir archivo), 4 (Inyección XSS/Script/HTML), 8 (Ejecución de comandos/Shell remoto) y 9 (Inyección SQL) de Tuning para este análisis, ya que son las que más juego pueden dar.

Realizamos el análisis:



```
┌──(kali㉿kali)-[~]
└─$ nikto -Tuning 0489 -host http://192.168.56.9/phpMyAdmin/import > analisis_linux.txt

┌──(kali㉿kali)-[~]
└─$ cat analisis_linux.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.9
+ Target Hostname:    192.168.56.9
+ Target Port:        80
+ Start Time:         2024-03-10 15:11:44 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /phpMyAdmin/import/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /phpMyAdmin/import/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /phpMyAdmin/import/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vu
lnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /phpMyAdmin/import: Uncommon header 'tcn' found, with contents: choice.
+ Multiple index files found: /phpMyAdmin/import/index.html, /phpMyAdmin/import/index.jsp, /phpMyAdmin/import/index.pl, /phpMyAdmin/import/index.do, /phpMyAdmin/import/index.cgi, /phpMyAdmin/import/default.aspx, /phpMyAdmin/import/defau
lt.asp, /phpMyAdmin/import/index.cfm, /phpMyAdmin/import/index.php7, /phpMyAdmin/import/index.php4, /phpMyAdmin/import/index.htm, /phpMyAdmin/import/index.php, /phpMyAdmin/import/index.aspx, /phpMyAdmin/import/index.shtml, /phpMyAdmin/i
mport/index.asp, /phpMyAdmin/import/index.php3, /phpMyAdmin/import/index.xml, /phpMyAdmin/import/index.jhtml, /phpMyAdmin/import/default.htm, /phpMyAdmin/import/index.php5.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /192.168.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /19216856.zip: Potentially interesting backup/cert file found. (NOTE: requested by IP address). See: https://cwe.mitre.org/data/definitions/530.html
+ /192168.tar.gz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /56.alz: Potentially interesting backup/cert file found. (NOTE: requested by IP address). See: https://cwe.mitre.org/data/definitions/530.html
+ /9.tar.lzma: Potentially interesting backup/cert file found. (NOTE: requested by IP address). See: https://cwe.mitre.org/data/definitions/530.html
+ /site.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /168.sql: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
```

La salida del comando anterior es extensa y llevaría tiempo analizarla. Con Cyberchef, podemos formatearla para que indique claramente las CVE :



gchq.github.io/CyberChef/#recipe=Regular_expression('User%20defined','CVE-%5B0-9%5D%7B4%7D-%5B0-9%5D*',true,true,false,false,false,false,'List%20matches')Unique('Line%20f...

Regular expression

Built in regexes: User defined

Regex: CVE-[0-9]{4}-[0-9]*

☑ Case insensitive ☑ ^ and $ match at newlines

□ Dot matches all □ Unicode support

□ Astral support □ Display total Output format: List matches

Unique

Delimiter: Line feed □ Display count

☑ Auto Bake

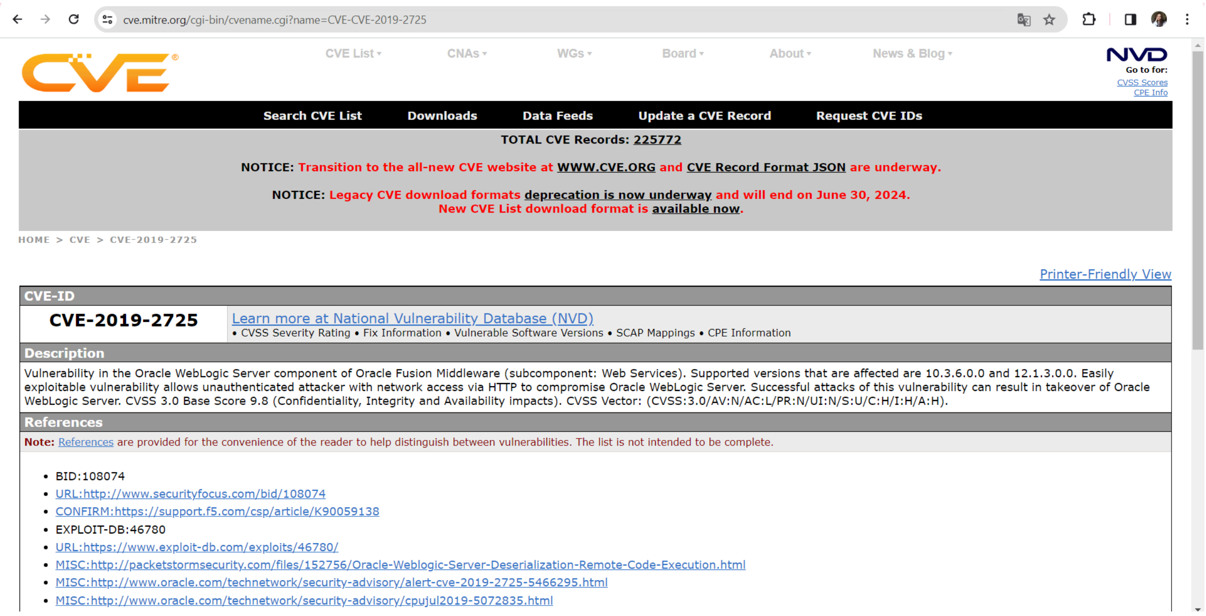
```
+ /phpMyAdmin/import/wls-wsat/CoordinatorPortType11: Oracle WebLogic Server may be vulnerable to
remote takeover. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271
+ /phpMyAdmin/import/wls-wsat/RegistrationPortTypeRPC11: Oracle WebLogic Server may be
vulnerable to remote takeover. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271

+ /phpMyAdmin/import/wls-wsat/ParticipantPortType11: Oracle WebLogic Server may be vulnerable to
remote takeover. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271
+ /phpMyAdmin/import/_async/AsyncResponseServiceJms?WSDL: BEA WebLogic may allow remote
takeover. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2725 CNVD-C-2019-48814
+ 1557 requests: 0 error(s) and 366 item(s) reported on remote host
+ End Time:           2024-03-10 15:13:23 (GMT-4) (99 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

abc 57520 ☰ 380 Raw Bytes LF

```
CVE-2003-1253
CVE-2001-0614
CVE-2003-0104
CVE-2002-0308
CVE-2006-6795
CVE-2002-1499
CVE-2002-1724
CVE-2003-1145
CVE-2002-1053
CVE-2002-0436
CVE-1999-0039
CVE-1999-0279
CVE-2002-0490
CVE-2002-0599
```

abc 336 ☰ 24 4ms Raw Bytes LF

Una vez que obtenemos las CVE, gracias a la web https://cve.mitre.org/ (página oficial del Mitre) podemos buscar las vulnerabilidades e indicar de qué tratan:



TOTAL CVE Records: 225772

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE download formats deprecation is now underway and will end on June 30, 2024.
New CVE List download format is available now.

HOME > CVE > CVE-2019-2725

Printer-Friendly View

CVE-ID

CVE-2019-2725 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:108074
- URL:http://www.securityfocus.com/bid/108074
- CONFIRM:https://support.f5.com/csp/article/K90059138
- EXPLOIT-DB:46780
- URL:https://www.exploit-db.com/exploits/46780/
- MISC:http://packetstormsecurity.com/files/152756/Oracle-Weblogic-Server-Deserialization-Remote-Code-Execution.html
- MISC:http://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html
- MISC:http://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

A continuación, se presenta un cuadro con las CVE encontradas para cada máquina:

CVE	Vulnerabilidad	Herramienta	Máquina
CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	OPENVAS	Windows
CVE-1999-0618	The rexec service is running	OPENVAS	Linux
CVE-2008-5304 CVE-2008-5305	TWiki XSS and Command Execution Vulnerabilities	OPENVAS	Linux
CVE-2001-0645 CVE-2004-2357 CVE-2006-1451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-3419 CVE-2015-4669 CVE-2016-6531 CVE-2018-15719	MySQL / MariaDB Default Credentials (MySQL Protocol)	OPENVAS	Linux

CVE	Vulnerabilidad	Herramienta	Máquina
CVE-2011-2523	vsftpd Compromised Source Packages Backdoor Vulnerability	OPENVAS	Linux
CVE-2020-1938	Apache Tomcat AJP RCE Vulnerability (Ghostcat)	OPENVAS	Linux
CVE-2004-2687	DistCC RCE Vulnerability (CVE-2004-2687)	OPENVAS	Linux
CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335	PHP-CGI-based setups vulnerability when parsing query string parameters from php...	OPENVAS	Linux
CVE-1999-0651	rsh Unencrypted Cleartext Login	OPENVAS	Linux
CVE-2011-3556	Java RMI Server Insecure Default Configuration RCE Vulnerability	OPENVAS	Linux
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2001-1594 CVE-2013-7404 CVE-2017-8218 CVE-2018-19063 CVE-2018-19064	FTP Brute Force Logins Reporting	OPENVAS	Linux
CVE-1999-0651	The rlogin service is running	OPENVAS	Linux
CVE-2014-0224	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	OPENVAS	Linux
CVE-2011-0411 CVE-2011-1430 CVE-2011-1431 CVE-2011-1432 CVE-2011-1506 CVE-2011-1575 CVE-2011-1926 CVE-2011-2165	Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	OPENVAS	Linux
CVE-2009-4898	TWiki Cross-Site Request Forgery	OPENVAS	Linux

CVE	Vulnerabilidad	Herramienta	Máquina
	Vulnerability (Sep 2010)		
CVE-1999-0497	Anonymous FTP Login Reporting	OPENVAS	Linux
CVE-2012-6708	jQuery < 1.9.0 XSS Vulnerability	OPENVAS	Linux
CVE-2018-20212	TWiki < 6.1.0 XSS Vulnerability	OPENVAS	Linux
CVE-2009-1339	TWiki Cross-Site Request Forgery Vulnerability	OPENVAS	Linux
CVE-2007-2447	Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check	OPENVAS	Linux
CVE-2016-0800 CVE-2014-3566	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	OPENVAS	Linux
CVE-2013-2566 CVE-2015-2808 CVE-2015-4000	SSL/TLS: Report Weak Cipher Suites	OPENVAS	Linux
CVE-2003-1567 CVE-2004-2320 CVE-2004-2763 CVE-2005-3398 CVE-2006-4683 CVE-2007-3008 CVE-2008-7253 CVE-2009-2823 CVE-2010-0386 CVE-2012-2223 CVE-2014-7883	HTTP Debugging Methods (TRACE/TRACK) Enabled	OPENVAS	Linux
CVE-2008-0149 CVE-2023-49282 CVE-2023-49283	phpinfo() Output Reporting (HTTP)	OPENVAS	Linux
CVE-2011-1473 CVE-2011-5094	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	OPENVAS	Linux
CVE-1999-0678	/doc directory browsable	OPENVAS	Linux

CVE	Vulnerabilidad	Herramienta	Máquina
CVE-2005-0283	QWikiwiki directory traversal vulnerability	OPENVAS	Linux
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	OPENVAS	Linux
CVE-2015-0204	SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	OPENVAS	Linux
CVE-2010-4480	phpMyAdmin 'error.php' Cross Site Scripting Vulnerability	OPENVAS	Linux
CVE-2011-4969	jQuery < 1.6.3 XSS Vulnerability	OPENVAS	Linux
CVE-2012-0053	Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	OPENVAS	Linux
CVE-2015-4000	SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)	OPENVAS	Linux
CVE-2014-3566	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	OPENVAS	Linux
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	OPENVAS	Linux
CVE-2003-1253	PHP remote file inclusion vulnerability in Bookmark4U 1.8.3 allows remote attackers to execute arbitrary PHP code viaa URL in the prefix parameter to (1) dbase.php, (2) config.php, or (3) common.load.php.	NIKTO	Linux
CVE-2001-0614	Carello E-Commerce 1.2.1 and earlier allows a remote attacker to gain additional privileges and execute arbitrary commands via a specially constructed URL.	NIKTO	Linux

CVE	Vulnerabilidad	Herramienta	Máquina
CVE-2003-0104	Directory traversal vulnerability in PeopleTools 8.10 through 8.18, 8.40, and 8.41 allows remote attackers to overwrite arbitrary files via the SchedulerTransfer servlet.	NIKTO	Linux
CVE-2002-0308	admin.asp in AdMentor 2.11 allows remote attackers to bypass authentication and gain privileges via a SQL injection attack on the Login and Password arguments.	NIKTO	Linux
CVE-2006-6795	PHP remote file inclusion vulnerability in gallery/displayCategory.php in the My_eGallery 2.5.6 module in myPHPNuke (MPN) allows remote attackers to execute arbitrary PHP code via a URL in the basepath parameter.	NIKTO	Linux
CVE-2002-1499	Multiple SQL injection vulnerabilities in FactoSystem CMS allows remote attackers to perform unauthorized database actions via (1) the authornumber parameter in author.asp, (2) the discussblurbid parameter in discuss.asp, (3) the name parameter in holdcomment.asp, and (4) the email parameter in holdcomment.asp.	NIKTO	Linux
CVE-2002-1724	Cross-site scripting vulnerability (XSS) in phpimageview.php for PHPImageView 1.0 allows remote attackers to execute arbitrary script as other users via the pic parameter.	NIKTO	Linux
CVE-2003-1145	Cross-site scripting (XSS) vulnerability in friendmail.php in OpenAutoClassifieds 1.0 allows remote attackers to inject arbitrary web script or HTML via the listing parameter.	NIKTO	Linux
CVE-2002-1053	Cross-site scripting (XSS)	NIKTO	Linux

CVE	Vulnerabilidad	Herramienta	Máquina
	vulnerability in W3C Jigsaw Proxy Server before 2.2.1 allows remote attackers to execute arbitrary script via a URL that contains a reference to a nonexistent host followed by the script, which is included in the resulting error message.		
CVE-2002-0436	sscd_suncourier.pl CGI script in the Sun Sunsolve CD pack allows remote attackers to execute arbitrary commands via shell metacharacters in the email address parameter.	NIKTO	Linux
CVE-1999-0039	webdist CGI program (webdist.cgi) in SGI IRIX allows remote attackers to execute arbitrary commands via shell metacharacters in the distloc parameter.	NIKTO	Linux
CVE-1999-0279	Excite for Web Servers (EWS) allows remote command execution via shell metacharacters.	NIKTO	Linux
CVE-2002-0490	Instant Web Mail before 0.60 does not properly filter CR/LF sequences, which allows remote attackers to (1) execute arbitrary POP commands via the id parameter in message.php, or (2) modify certain mail message headers via numerous parameters in write.php.	NIKTO	Linux
CVE-2002-0599	Blahz-DNS 0.2 and earlier allows remote attackers to bypass authentication and modify configuration by directly requesting CGI programs such as dostuff.php instead of going through the login screen.	NIKTO	Linux
CVE-2002-0220	phpsmssend.php in PhpSmsSend 1.0 allows remote attackers to execute arbitrary commands via an SMS message	NIKTO	Linux

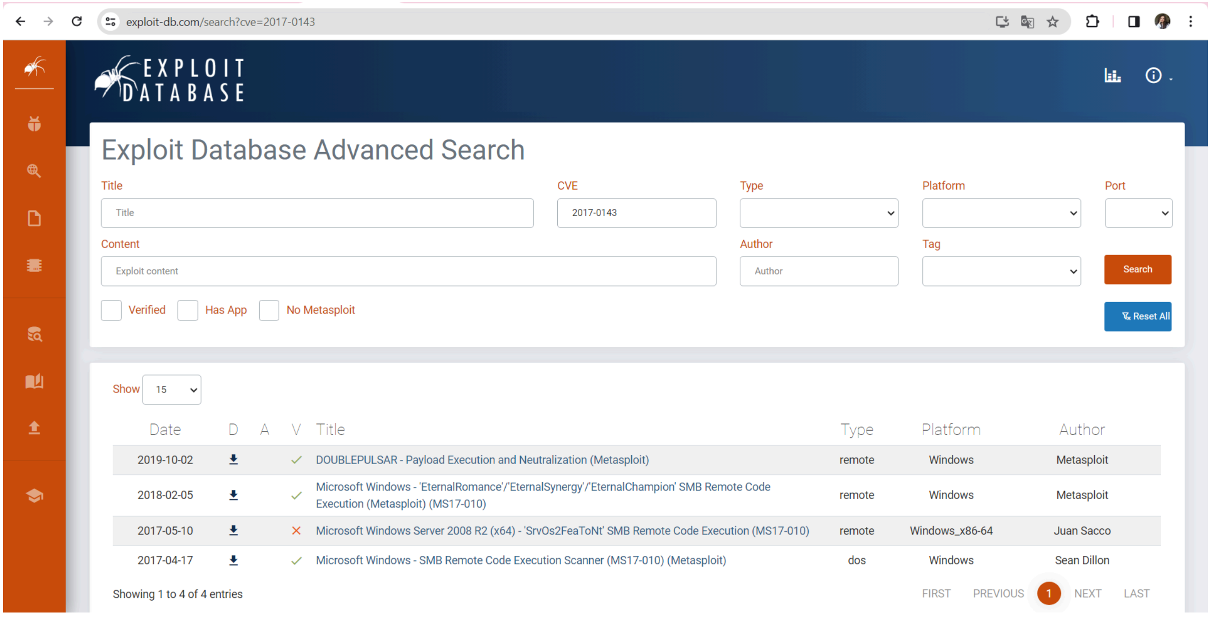
CVE	Vulnerabilidad	Herramienta	Máquina
	containing shell metacharacters.		
CVE-2001-0537	HTTP server for Cisco IOS 11.3 to 12.2 allows attackers to bypass authentication and execute arbitrary commands, when local authorization is being used, by specifying a high access level in the URL.	NIKTO	Linux
CVE-2003-0560	SQL injection vulnerability in shopexd.asp for VP-ASP allows remote attackers to gain administrator privileges via the id parameter.	NIKTO	Linux
CVE-1999-1011	The Remote Data Service (RDS) DataFactory component of Microsoft Data Access Components (MDAC) in IIS 3.x and 4.x exposes unsafe methods, which allows remote attackers to execute arbitrary commands.	NIKTO	Linux
CVE-2000-0628	The source.asp example script in the Apache ASP module Apache::ASP 1.93 and earlier allows remote attackers to modify files	NIKTO	Linux
CVE-2002-0579	WorkforceROI Xpede 4.1 allows remote attackers to gain privileges as an Xpede administrator via a direct HTTP request to the /admin/adminproc.asp script, which does not prompt for a password.	NIKTO	Linux
CVE-2012-1823	sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt	NIKTO	Linux

CVE	Vulnerabilidad	Herramienta	Máquina
	for the 'd' case.		
CVE-2014-3704	The expandArguments function in the database abstraction API in Drupal core 7.x before 7.32 does not properly construct prepared statements, which allows remote attackers to conduct SQL injection attacks via an array containing crafted keys.	NIKTO	Linux
CVE-2017-10271	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Security). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.	NIKTO	Linux
CVE-2019-2725	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.	NIKTO	Linux

La tabla cuenta con vulnerabilidades que van desde gravedad alta hasta gravedad baja, por lo que podriamos causar un gran impacto en los sistemas aprovechando algunas de ellas. Por ejemplo: CVE-2017-0143, CVE-2020-1938, CVE-2017-10271, CVE-2019-2725, ...

2 - Identificación de Exploits

Entraremos en la web https://www.exploit-db.com, que ofrece una base de datos de exploits, utilizada por SearchExploit. Utilizaremos esta plataforma para buscar exploits correspondientes a las vulnerabilidades que hemos identificado previamente, para ello tenemos que indicar las CVE asociadas:



exploit-db.com/search?cve=2017-0143

EXPLOIT DATABASE

Exploit Database Advanced Search

Title: Title
CVE: 2017-0143
Type:
Platform:
Port:
Content: Exploit content
Author: Author
Tag:

Search

□ Verified □ Has App □ No Metasploit

Reset All

Show 15

Date	D	A	V	Title	Type	Platform	Author
2019-10-02	⬇		✓	DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)	remote	Windows	Metasploit
2018-02-05	⬇		✓	Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010)	remote	Windows	Metasploit
2017-05-10	⬇		✗	Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)	remote	Windows_x86-64	Juan Sacco
2017-04-17	⬇		✓	Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)	dos	Windows	Sean Dillon

Showing 1 to 4 of 4 entries

FIRST PREVIOUS 1 NEXT LAST

A continuación, presentaremos los resultados obtenidos. Se ha indicado la vulnerabilidad en vez de el CVE dado que hay grupos de CVE asociados a una misma vulnerabilidad pero que no comparten el mismo exploit:

Vulnerabilidad	Exploit
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	https://www.exploit-db.com/exploits/47456 DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit) (exploit automático) https://www.exploit-db.com/exploits/41987 Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) (exploit manual)
The rexec service is running	No hay datos disponibles en la base de datos.
TWiki XSS and Command Execution Vulnerabilities	https://www.exploit-db.com/exploits/32646 TWiki 4.x - 'URLPARAM' Cross-Site Scripting (exploit manual)

MySQL / MariaDB Default Credentials (MySQL Protocol)	https://www.exploit-db.com/exploits/37708 Xceedium Xsuite - Multiple Vulnerabilities (exploit manual)
vsftpd Compromised Source Packages Backdoor Vulnerability	https://www.exploit-db.com/exploits/49757 vsftpd 2.3.4 - Backdoor Command Execution (exploit manual) https://www.exploit-db.com/exploits/17491 (exploit automático)
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	https://www.exploit-db.com/exploits/49039 Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit) (exploit automático) https://www.exploit-db.com/exploits/48143 Apache Tomcat - AJP 'Ghostcat File Read/Inclusion (exploit manual)
DistCC RCE Vulnerability (CVE-2004-2687)	https://www.exploit-db.com/exploits/9915 DistCC Daemon - Command Execution (Metasploit) (exploit automático)
PHP-CGI-based setups vulnerability when parsing query string parameters from php...	https://www.exploit-db.com/exploits/18834 PHP 5.3.12/5.4.2 - CGI Argument Injection (Metasploit) (exploit automático) https://www.exploit-db.com/exploits/18836 PHP < 5.3.12 / < 5.4.2 - CGI Argument Injection (exploit manual)
rsh Unencrypted Cleartext Login	No hay datos disponibles en la base de datos.
Java RMI Server Insecure Default Configuration RCE Vulnerability	https://www.exploit-db.com/exploits/17535 Java RMI - Server Insecure Default Configuration Java Code Execution (Metasploit) (exploit automático)
FTP Brute Force Logins Reporting	https://www.exploit-db.com/exploits/41694 SSH - User Code Execution (Metasploit) (exploit automático)
The rlogin service is running	No hay datos disponibles en la base de datos.

SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	No hay datos disponibles en la base de datos.
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	https://www.exploit-db.com/exploits/37440 Watchguard XCS 10.0 - Multiple Vulnerabilities (exploit manual)
TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)	No hay datos disponibles en la base de datos.
Anonymous FTP Login Reporting	No hay datos disponibles en la base de datos.
jQuery < 1.9.0 XSS Vulnerability	https://www.exploit-db.com/exploits/49708 Linksys EA7500 2.0.8.194281 - Cross-Site Scripting (exploit manual)
TWiki < 6.1.0 XSS Vulnerability	No hay datos disponibles en la base de datos.
TWiki Cross-Site Request Forgery Vulnerability	No hay datos disponibles en la base de datos.
Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check	https://www.exploit-db.com/exploits/16320 Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) (exploit automático)
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	No hay datos disponibles en la base de datos.

SSL/TLS: Report Weak Cipher Suites	No hay datos disponibles en la base de datos.
HTTP Debugging Methods (TRACE/TRACK) Enabled	https://www.exploit-db.com/exploits/35982 Hewlett-Packard (HP) UCMDB - JMX-Console Authentication Bypass (exploit manual)
phpinfo() Output Reporting (HTTP)	https://www.exploit-db.com/exploits/4861 TUTOS 1.3 - 'cmd.php' Remote Command Execution (exploit manual)
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	No hay datos disponibles en la base de datos.
/doc directory browsable	https://www.exploit-db.com/exploits/19253 Debian 2.1 - HTTPd (exploit manual)
QWikiwiki directory traversal vulnerability	https://www.exploit-db.com/exploits/737 QwikiWiki - Directory Traversal (exploit manual)
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	No hay datos disponibles en la base de datos.
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	No hay datos disponibles en la base de datos.
phpMyAdmin 'error.php' Cross Site Scripting Vulnerability	https://www.exploit-db.com/exploits/15699 phpMyAdmin - Client-Side Code Injection / Redirect Link Falsification (exploit manual)

jQuery < 1.6.3 XSS Vulnerability	No hay datos disponibles en la base de datos.
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	https://www.exploit-db.com/exploits/18442 Apache - httpOnly Cookie Disclosure (exploit manual)
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)	No hay datos disponibles en la base de datos.
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	No hay datos disponibles en la base de datos.
ICMP Timestamp Reply Information Disclosure	No hay datos disponibles en la base de datos.
PHP remote file inclusion vulnerability in Bookmark4U 1.8.3 allows remote attackers to execute arbitrary PHP code viaa URL in the prefix parameter to (1) dbase.php, (2) config.php, or (3) common.load.p	No hay datos disponibles en la base de datos.

hp.	
Carello E-Commerce 1.2.1 and earlier allows a remote attacker to gain additional privileges and execute arbitrary commands via a specially constructed URL.	https://www.exploit-db.com/exploits/20850 Pacific Software Carello 1.2.1 Shopping Cart - Command Execution (exploit manual)
Directory traversal vulnerability in PeopleTools 8.10 through 8.18, 8.40, and 8.41 allows remote attackers to overwrite arbitrary files via the SchedulerTransfer servlet.	No hay datos disponibles en la base de datos.
admin.asp in AdMentor 2.11 allows remote attackers to bypass authentication and gain privileges via a SQL injection attack on the Login and Password arguments.	No hay datos disponibles en la base de datos.
PHP remote file inclusion vulnerability in gallery/displayCategory.php in the My_eGallery 2.5.6 module in	https://www.exploit-db.com/exploits/3010 myPHPNuke Module My_eGallery 2.5.6 - 'basepath' Remote File Inclusion (exploit manual)

myPHPNuke (MPN) allows remote attackers to execute arbitrary PHP code via a URL in the basepath parameter.	
Multiple SQL injection vulnerabilities in FactoSystem CMS allows remote attackers to perform unauthorized database actions via (1) the authornumber parameter in author.asp, (2) the discussblurbid parameter in discuss.asp, (3) the name parameter in holdcomment.asp, and (4) the email parameter in holdcomment.asp.	https://www.exploit-db.com/exploits/21766 FactoSystem Weblog 0.9/1.0/1.1 - Multiple SQL Injections (exploit manual)
Cross-site scripting vulnerability (XSS) in phpimageview.php for PHPImageView 1.0 allows remote attackers to execute arbitrary script as other users	No hay datos disponibles en la base de datos.

via the pic parameter.	
Cross-site scripting (XSS) vulnerability in friendmail.php in OpenAutoClassifieds 1.0 allows remote attackers to inject arbitrary web script or HTML via the listing parameter.	https://www.exploit-db.com/exploits/23336 OpenAutoClassifieds 1.0 - 'Listing' Cross-Site Scripting (exploit manual)
Cross-site scripting (XSS) vulnerability in W3C Jigsaw Proxy Server before 2.2.1 allows remote attackers to execute arbitrary script via a URL that contains a reference to a nonexistent host followed by the script, which is included in the resulting error message.	No hay datos disponibles en la base de datos.
sscd_suncourier.pl CGI script in the Sun Sunsolve CD pack allows remote attackers to execute arbitrary commands via shell metacharacters in the email	https://www.exploit-db.com/exploits/21340 Solaris 7.0/8 Sunsolve CD - SSCD_SunCourier.pl CGI Script Arbitrary Command Execution (exploit manual)

address parameter.	
webdist CGI program (webdist.cgi) in SGI IRIX allows remote attackers to execute arbitrary commands via shell metacharacters in the distloc parameter.	https://www.exploit-db.com/exploits/19299 SGI IRIX 6.3 - cgi-bin 'webdist.cgi' Command Execution (exploit manual)
Excite for Web Servers (EWS) allows remote command execution via shell metacharacters.	No hay datos disponibles en la base de datos.
Instant Web Mail before 0.60 does not properly filter CR/LF sequences, which allows remote attackers to (1) execute arbitrary POP commands via the id parameter in message.php, or (2) modify certain mail message headers via numerous parameters in write.php.	No hay datos disponibles en la base de datos.
Blahz-DNS 0.2 and earlier allows remote	https://www.exploit-db.com/exploits/21426 Blahz-DNS 0.2 - Direct Script Call Authentication Bypass (exploit manual)

attackers to bypass authentication and modify configuration by directly requesting CGI programs such as dostuff.php instead of going through the login screen.	
phpsmssend.php in PhpSmsSend 1.0 allows remote attackers to execute arbitrary commands via an SMS message containing shell metacharacters.	No hay datos disponibles en la base de datos.
HTTP server for Cisco IOS 11.3 to 12.2 allows attackers to bypass authentication and execute arbitrary commands, when local authorization is being used, by specifying a high access level in the URL.	https://www.exploit-db.com/exploits/20975 Cisco IOS 11.x/12.x - HTTP Configuration Arbitrary Administrative Access (1) (exploit manual) https://www.exploit-db.com/exploits/20976 Cisco IOS 11.x/12.x - HTTP Configuration Arbitrary Administrative Access (2) (exploit manual)
SQL injection vulnerability in shopexd.asp for VP-ASP allows remote attackers to gain administrator privileges via the id	https://www.exploit-db.com/exploits/22888 Virtual Programming VP-ASP 5.00 - 'shopexd.asp' SQL Injection (1) (exploit manual) https://www.exploit-db.com/exploits/22889 Virtual Programming VP-ASP 5.00 - 'shopexd.asp' SQL Injection (2) (exploit manual)

parameter.	
The Remote Data Service (RDS) DataFactory component of Microsoft Data Access Components (MDAC) in IIS 3.x and 4.x exposes unsafe methods, which allows remote attackers to execute arbitrary commands.	https://www.exploit-db.com/exploits/19424 Microsoft Data Access Components (MDAC) 2.1 / Microsoft IIS 3.0/4.0 / Microsoft Index Server 2.0 / Microsoft Site Server Commerce Edition 3.0 i386 MDAC - RDS (1) (exploit manual) https://www.exploit-db.com/exploits/19425 Microsoft Data Access Components (MDAC) 2.1 / Microsoft IIS 3.0/4.0 / Microsoft Index Server 2.0 / Microsoft Site Server Commerce Edition 3.0 i386 MDAC - RDS (2) (exploit manual)
The source.asp example script in the Apache ASP module Apache::ASP 1.93 and earlier allows remote attackers to modify files	No hay datos disponibles en la base de datos.
WorkforceROI Xpede 4.1 allows remote attackers to gain privileges as an Xpede administrator via a direct HTTP request to the /admin/adminproc.asp script, which does not prompt for a password.	No hay datos disponibles en la base de datos.
sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a	

CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.	
sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.	https://www.exploit-db.com/exploits/18834 PHP 5.3.12/5.4.2 - CGI Argument Injection (Metasploit) (exploit automático) https://www.exploit-db.com/exploits/18836 (exploit manual)
The	https://www.exploit-db.com/exploits/34984 Drupal 7.0 < 7.31 -

expandArguments function in the database abstraction API in Drupal core 7.x before 7.32 does not properly construct prepared statements, which allows remote attackers to conduct SQL injection attacks via an array containing crafted keys.	'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1) (exploit manual) https://www.exploit-db.com/exploits/35150 Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution) (exploit manual)
Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Security). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in	https://www.exploit-db.com/exploits/43924 Oracle WebLogic - wls-wsat Component Deserialization Remote Code Execution (Metasploit) (exploit automático) https://www.exploit-db.com/exploits/43458 Oracle WebLogic < 10.3.6 - 'wls-wsat' Component Deserialisation Remote Command Execution (exploit manual)

takeover of Oracle WebLogic Server.	
Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.	https://www.exploit-db.com/exploits/46814 Oracle Weblogic Server - 'AsyncResponseService' Deserialization Remote Code Execution (Metasploit) (exploit automático)