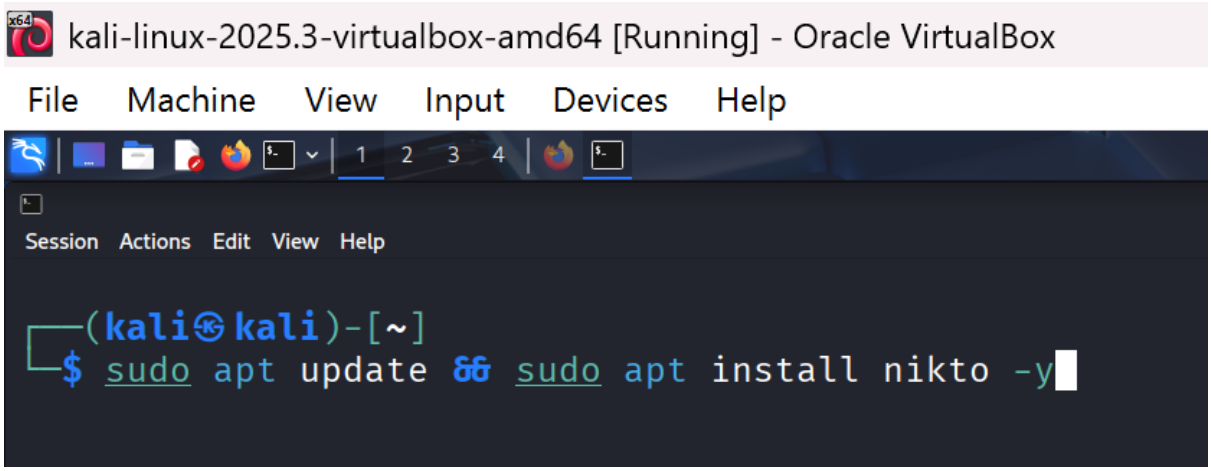
TASK-7 VULNERABILITY SCANNING WITH NIKTO

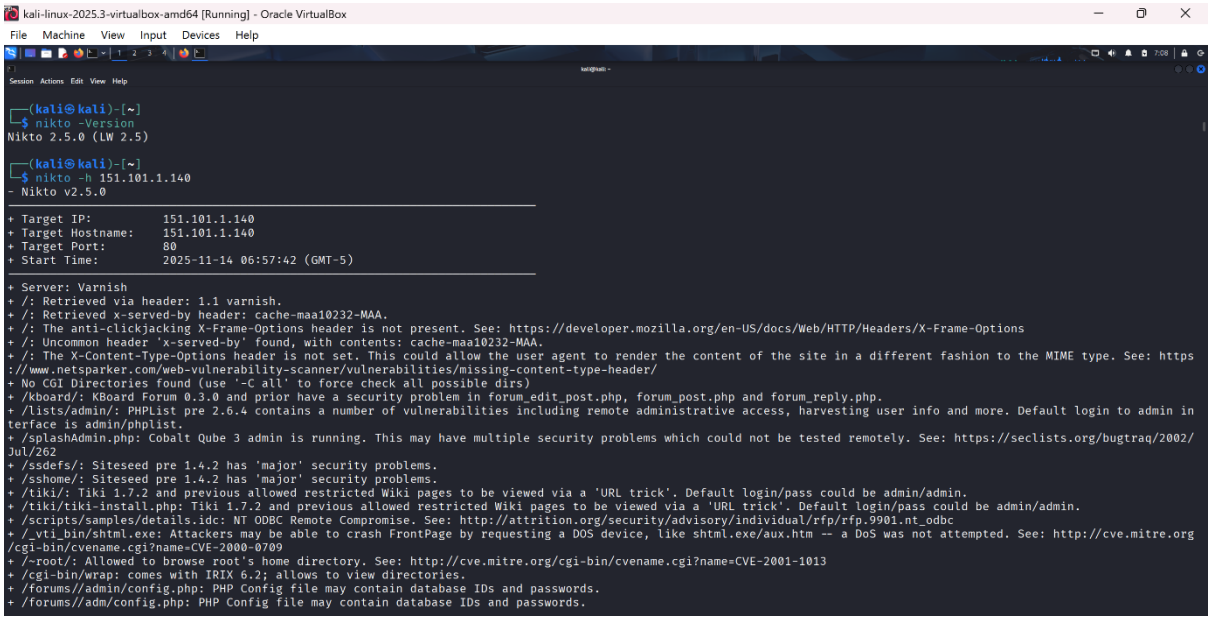
Step 1: Install nikto by using the following command:



Step 2: Check the version of the nikto, if it's the latest version.

Step 3: Get the IP address of the targeted sited and then execute the following command

"nikto -h <targeted ip address>"



kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
+ /scripts/tools/ctss.idc: This CGI allows remote users to view and modify SQL DB contents, server paths, docroot and more.
+ /bigconf.cgi: BigIP Configuration CGI.
+ /vgn/style: Vignette server may reveal system information through this file. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0401
+ /SiteServer/Admin/commerce/foundation/domain.asp: Displays known domains of which that server is involved. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1769
+ /SiteServer/Admin/commerce/foundation/driver.asp: Displays a list of installed ODBC drivers. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1769
+ /SiteServer/Admin/commerce/foundation/DSN.asp: Displays all DSNs configured for selected ODBC drivers. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1769
+ /SiteServer/admin/findvserver.asp: Gives a list of installed Site Server components. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1769
+ /SiteServer/Admin/knowledge/dsmgr/default.asp: Used to view current search catalog configurations.
+ /basilix/mbox-list.php3: BasiliX webmail application prior to 1.1.1 contains a XSS issue in 'message list' function/page.
+ /basilix/message-read.php3: BasiliX webmail application prior to 1.1.1 contains a XSS issue in 'read message' function/page.
+ /clusterframe.jsp: Macromedia JRun 4 build 61650 remote administration interface is vulnerable to several XSS attacks.
+ /IlohaMail/blank.html: IlohaMail 0.8.10 contains a XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /bb-dnbd/faxsurvey: This may allow arbitrary command execution.
+ /cartcart.cgi: If this is Dansie Shopping Cart 3.0.8 or earlier, it contains a backdoor to allow attackers to execute arbitrary commands.
+ /scripts/Carello/Carello.dll: Carello 1.3 may allow commands to be executed on the server by replacing hidden form elements. This could not be tested by Nikto. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0614
+ /scripts/tools/dsnform.exe: Allows creation of ODBC Data Source.
+ /scripts/tools/dsnform: Allows creation of ODBC Data Source.
+ /SiteServer/Admin/knowledge/dsmgr/users/GroupManager.asp: Microsoft Site Server script used to create, modify, and potentially delete LDAP users and groups. See: https://securitytracker.com/id/1003420
+ /SiteServer/Admin/knowledge/dsmgr/users/UserManager.asp: Microsoft Site Server used to create, modify, and potentially delete LDAP users and groups. See: https://securitytracker.com/id/1003420
+ /prd.i/pgen/: Has MS Merchant Server 1.0.
+ /readme.eml: Remote server may be infected with the Nimda virus.
+ /scripts/httpodbc.dll: Possible IIS backdoor found.
+ /scripts/proxy/w3proxy.dll: MSProxy v1.0 installed.
+ /SiteServer/admin/: Site Server components admin. Default account may be 'LDAP_Anonymous', pass is 'LdapPassword_1'. See: https://github.com/sullo/advisory-archives/blob/master/RFP2201.txt
+ /siteseed/: Siteseed pre 1.4.2 have 'major' security problems.
+ /pccsmysqladm/incs/dbconnect.inc: This file should not be accessible, as it contains database connectivity information. Upgrade to version 1.2.5 or higher.
+ /iisadmin/: Access to /iisadmin should be restricted to localhost or allowed hosts only.
+ /PDG_Cart/order.log: PDG Commerce log found. See: http://zodi.com/cgi-bin/shopper.cgi?display=intro&template=Intro/commerce.html
+ /ows/restricted%2eshow: OWS may allow restricted files to be viewed by replacing a character with its encoded equivalent.
+ /view_source.jsp: Resin 2.1.2 view_source.jsp allows any file on the system to be viewed by using \..\ directory traversal. This script may be vulnerable.
+ /w-agora/: w-agora pre 4.1.4 may allow a remote user to execute arbitrary PHP scripts via URL includes in include/*.php and user/*.php files. Default account is 'admin' but password set during install.
```

Right Ctrl

kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox

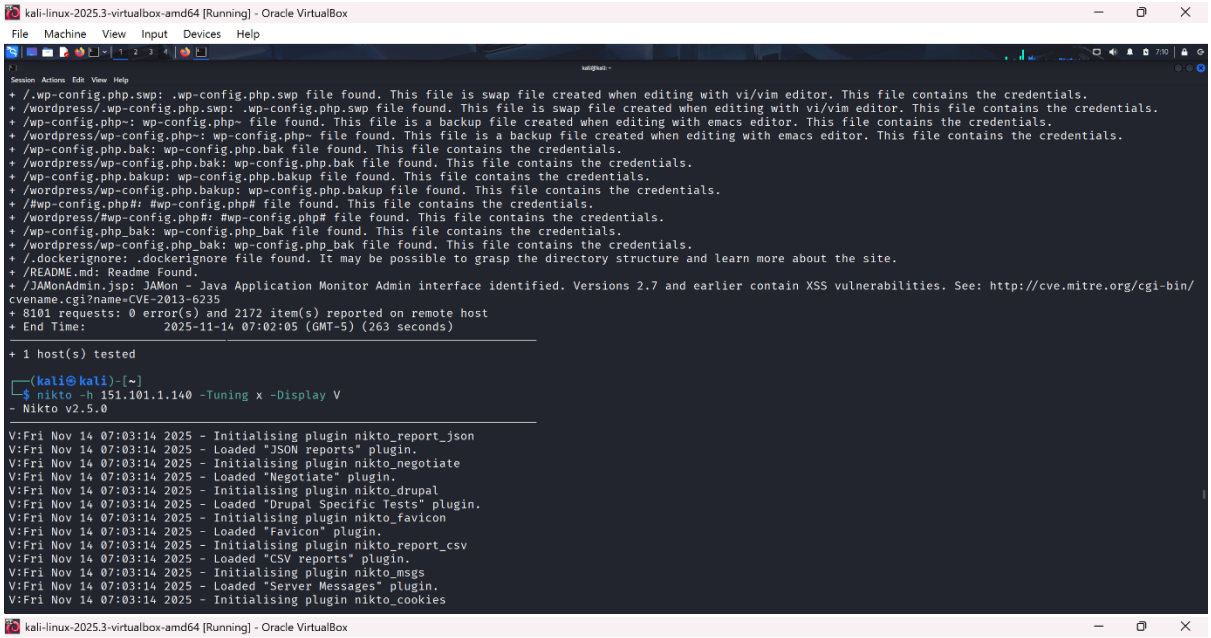
File Machine View Input Devices Help

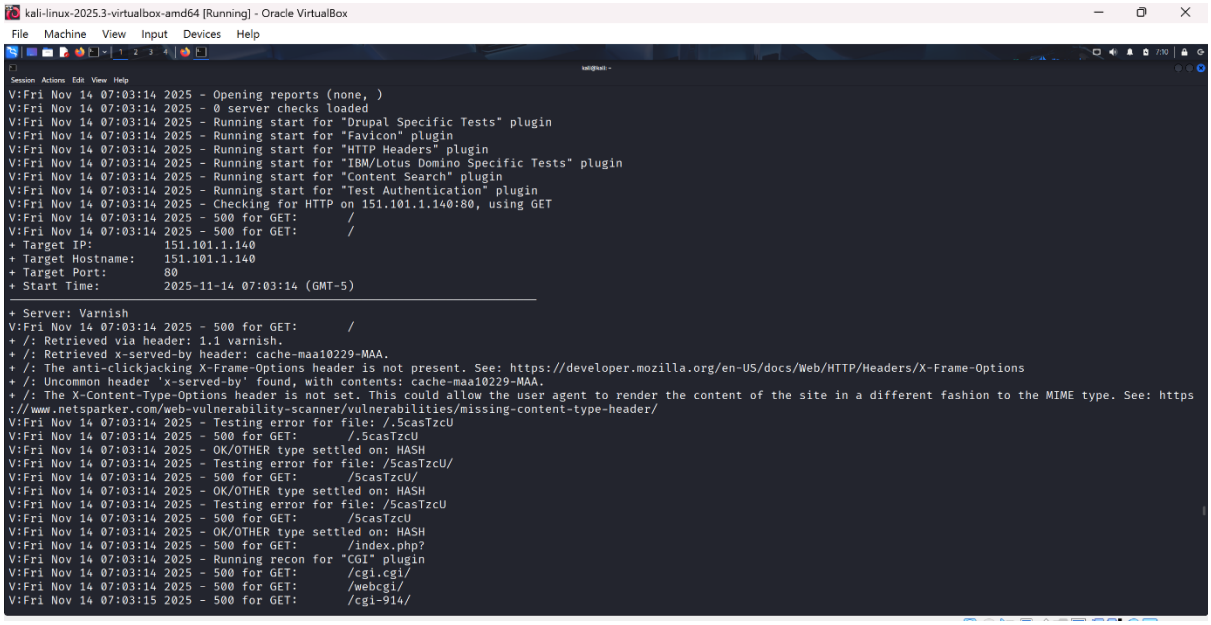
```
nd running .bas files on server.
+ /nsn/..%5Cutil/copy.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/del.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/dir.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/dsbrowse.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/glist.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/lancard.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/md.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/rd.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/ren.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/send.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/set.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/slist.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/type.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cutil/userlist.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cweb/env.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cweb/fdir.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cwebdemo/env.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /nsn/..%5Cwebdemo/fdir.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server.
+ /upd/: WASD Server can allow directory listings by requesting /upd/directory/. Upgrade to a later version and secure according to the documents on the WASD web site.
```

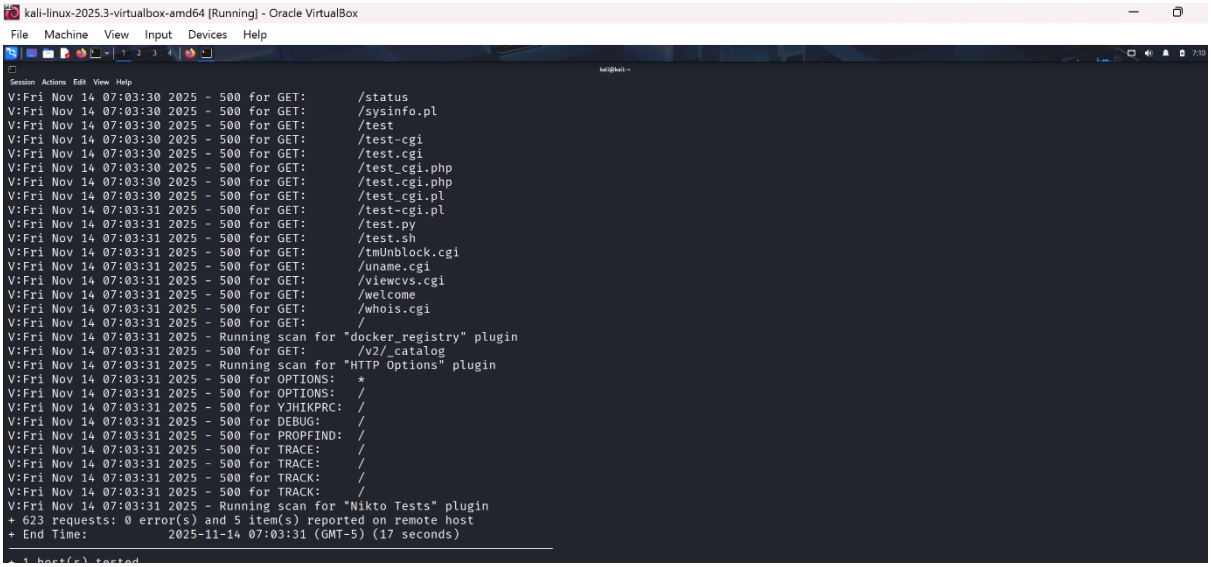
kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox

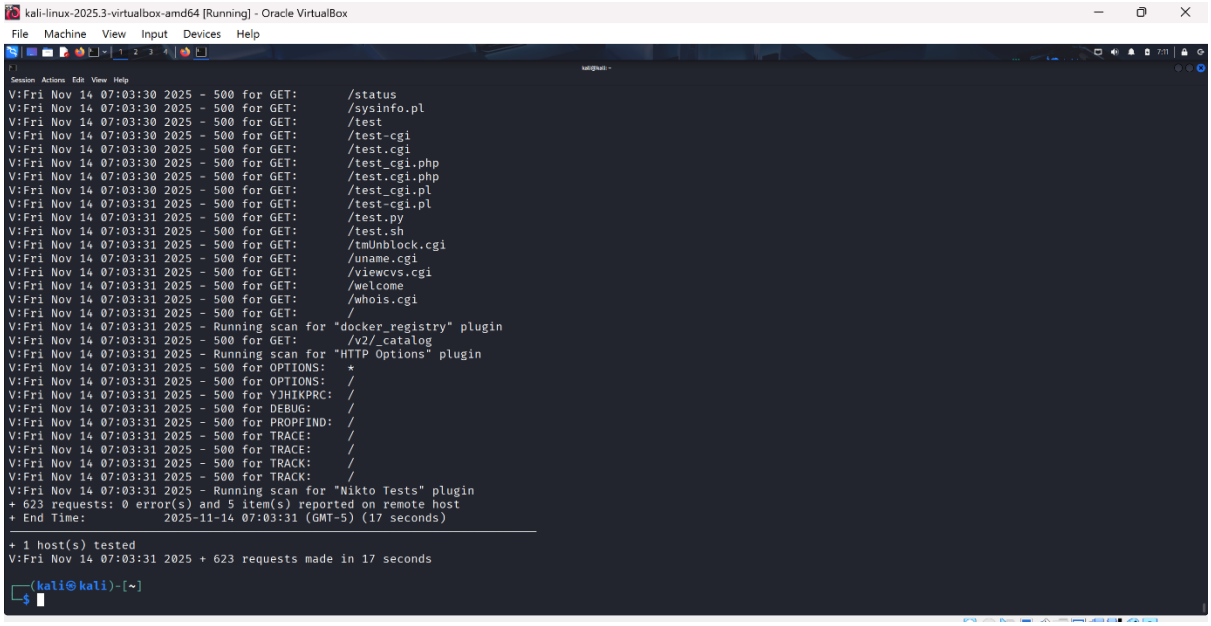
File Machine View Input Devices Help

```
+ /config/readme.txt: Readme file found.
+ /data/readme.txt: Readme file found.
+ /log/readme.txt: Readme file found.
+ /logs/readme.txt: Readme file found.
+ /uploads/readme.txt: Readme file found.
+ /admin1.php: Admin login page found.
+ /admin.asp: Admin login page/section found.
+ /admin/account.asp: Admin login page/section found.
+ /admin/account.html: Admin login page/section found.
+ /admin/account.php: Admin login page/section found.
+ /admin/controlpanel.asp: Admin login page/section found.
+ /admin/controlpanel.html: Admin login page/section found.
+ /admin/controlpanel.php: Admin login page/section found.
+ /admin/cp.asp: Admin login page/section found.
+ /admin/cp.html: Admin login page/section found.
+ /admin/cp.php: Admin login page/section found.
+ /admin/home.asp: Admin login page/section found.
+ /admin/home.php: Admin login page/section found.
+ /admin/index.asp: Admin login page/section found.
+ /admin/index.html: Admin login page/section found.
+ /admin/login.asp: Admin login page/section found.
+ /admin/login.html: Admin login page/section found.
+ /admin/login.php: Admin login page/section found.
+ /admin1.asp: Admin login page/section found.
+ /admin1.html: Admin login page/section found.
+ /admin1/: Admin login page/section found.
+ /admin2.asp: Admin login page/section found.
+ /admin2.html: Admin login page/section found.
+ /admin2.php: Admin login page/section found.
+ /admin4_account/: Admin login page/section found.
+ /admin4_colon/: Admin login page/section found.
+ /admincontrol.asp: Admin login page/section found.
+ /admincontrol.html: Admin login page/section found.
+ /admincontrol.php: Admin login page/section found.
+ /administer/: Admin login page/section found.
+ /administr8.asp: Admin login page/section found.
+ /administr8.html: Admin login page/section found.
+ /administr8.php: Admin login page/section found.
```


kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
+ /.wp-config.php.swp: .wp-config.php.swp file found. This file is swap file created when editing with vi/vim editor. This file contains the credentials.
+ /wordpress/.wp-config.php.swp: .wp-config.php.swp file found. This file is swap file created when editing with vi/vim editor. This file contains the credentials.
+ /wp-config.php~: wp-config.php~ file found. This file is a backup file created when editing with emacs editor. This file contains the credentials.
+ /wordpress/wp-config.php~: wp-config.php~ file found. This file is a backup file created when editing with emacs editor. This file contains the credentials.
+ /wp-config.php.bak: wp-config.php.bak file found. This file contains the credentials.
+ /wordpress/wp-config.php.bak: wp-config.php.bak file found. This file contains the credentials.
+ /wp-config.php.bakup: wp-config.php.bakup file found. This file contains the credentials.
+ /wordpress/wp-config.php.bakup: wp-config.php.bakup file found. This file contains the credentials.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ /wordpress/#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ /wp-config.php_bak: wp-config.php_bak file found. This file contains the credentials.
+ /wordpress/wp-config.php_bak: wp-config.php_bak file found. This file contains the credentials.
+ /.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
+ /README.md: Readme Found.
+ /JAMonAdmin.jsp: JAMon - Java Application Monitor Admin interface identified. Versions 2.7 and earlier contain XSS vulnerabilities. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6235
+ 8101 requests: 0 error(s) and 2172 item(s) reported on remote host
+ End Time: 2025-11-14 07:02:05 (GMT-5) (263 seconds)
+ 1 host(s) tested
┌──(kali㉿kali)-[~]
└─$ nikto -h 151.101.1.140 -Tuning x -Display V
- Nikto v2.5.0
V:Fri Nov 14 07:03:14 2025 - Initialising plugin nikto_report_json
V:Fri Nov 14 07:03:14 2025 - Loaded "JSON reports" plugin.
V:Fri Nov 14 07:03:14 2025 - Initialising plugin nikto_negotiate
V:Fri Nov 14 07:03:14 2025 - Loaded "Negotiate" plugin.
V:Fri Nov 14 07:03:14 2025 - Initialising plugin nikto_drupal
V:Fri Nov 14 07:03:14 2025 - Loaded "Drupal Specific Tests" plugin.
V:Fri Nov 14 07:03:14 2025 - Initialising plugin nikto_favicon
V:Fri Nov 14 07:03:14 2025 - Loaded "Favicon" plugin.
V:Fri Nov 14 07:03:14 2025 - Initialising plugin nikto_report_csv
V:Fri Nov 14 07:03:14 2025 - Loaded "CSV reports" plugin.
V:Fri Nov 14 07:03:14 2025 - Initialising plugin nikto_msgs
V:Fri Nov 14 07:03:14 2025 - Loaded "Server Messages" plugin.
V:Fri Nov 14 07:03:14 2025 - Initialising plugin nikto_cookies


kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
V:Fri Nov 14 07:03:14 2025 - Opening reports (none,)
V:Fri Nov 14 07:03:14 2025 - 0 server checks loaded
V:Fri Nov 14 07:03:14 2025 - Running start for "Drupal Specific Tests" plugin
V:Fri Nov 14 07:03:14 2025 - Running start for "Favicon" plugin
V:Fri Nov 14 07:03:14 2025 - Running start for "HTTP Headers" plugin
V:Fri Nov 14 07:03:14 2025 - Running start for "IBM/Lotus Domino Specific Tests" plugin
V:Fri Nov 14 07:03:14 2025 - Running start for "Content Search" plugin
V:Fri Nov 14 07:03:14 2025 - Running start for "Test Authentication" plugin
V:Fri Nov 14 07:03:14 2025 - Checking for HTTP on 151.101.1.140:80, using GET
V:Fri Nov 14 07:03:14 2025 - 500 for GET: /
V:Fri Nov 14 07:03:14 2025 - 500 for GET: /
+ Target IP: 151.101.1.140
+ Target Hostname: 151.101.1.140
+ Target Port: 80
+ Start Time: 2025-11-14 07:03:14 (GMT-5)
+ Server: Varnish
V:Fri Nov 14 07:03:14 2025 - 500 for GET: /
+ /: Retrieved via header: 1.1 varnish.
+ /: Retrieved x-served-by header: cache-maa10229-MAA.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-served-by' found, with contents: cache-maa10229-MAA.
+ /: 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/vulnerabilities/missing-content-type-header/
V:Fri Nov 14 07:03:14 2025 - Testing error for file: /.5casTzcU
V:Fri Nov 14 07:03:14 2025 - 500 for GET: /.5casTzcU
V:Fri Nov 14 07:03:14 2025 - OK/OTHER type settled on: HASH
V:Fri Nov 14 07:03:14 2025 - Testing error for file: /5casTzcU/
V:Fri Nov 14 07:03:14 2025 - 500 for GET: /5casTzcU/
V:Fri Nov 14 07:03:14 2025 - OK/OTHER type settled on: HASH
V:Fri Nov 14 07:03:14 2025 - Testing error for file: /5casTzcU
V:Fri Nov 14 07:03:14 2025 - 500 for GET: /5casTzcU
V:Fri Nov 14 07:03:14 2025 - OK/OTHER type settled on: HASH
V:Fri Nov 14 07:03:14 2025 - 500 for GET: /index.php?
V:Fri Nov 14 07:03:14 2025 - Running recon for "CGI" plugin
V:Fri Nov 14 07:03:14 2025 - 500 for GET: /cgi.cgi/
V:Fri Nov 14 07:03:14 2025 - 500 for GET: /webcgi/
V:Fri Nov 14 07:03:15 2025 - 500 for GET: /cgi-914/


kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /status
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /sysinfo.pl
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /test
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /test-cgi
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /test.cgi
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /test_cgi.php
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /test.cgi.php
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /test_cgi.pl
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /test-cgi.pl
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /test.py
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /test.sh
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /tmUnblock.cgi
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /uname.cgi
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /viewcvs.cgi
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /welcome
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /whois.cgi
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /
V:Fri Nov 14 07:03:31 2025 - Running scan for "docker_registry" plugin
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /v2/_catalog
V:Fri Nov 14 07:03:31 2025 - Running scan for "HTTP Options" plugin
V:Fri Nov 14 07:03:31 2025 - 500 for OPTIONS: *
V:Fri Nov 14 07:03:31 2025 - 500 for OPTIONS: /
V:Fri Nov 14 07:03:31 2025 - 500 for YJHIKPRC: /
V:Fri Nov 14 07:03:31 2025 - 500 for DEBUG: /
V:Fri Nov 14 07:03:31 2025 - 500 for PROPFIND: /
V:Fri Nov 14 07:03:31 2025 - 500 for TRACE: /
V:Fri Nov 14 07:03:31 2025 - 500 for TRACE: /
V:Fri Nov 14 07:03:31 2025 - 500 for TRACK: /
V:Fri Nov 14 07:03:31 2025 - 500 for TRACK: /
V:Fri Nov 14 07:03:31 2025 - Running scan for "Nikto Tests" plugin
+ 623 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2025-11-14 07:03:31 (GMT-5) (17 seconds)


kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /status
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /sysinfo.pl
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /test
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /test-cgi
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /test.cgi
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /test_cgi.php
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /test.cgi.php
V:Fri Nov 14 07:03:30 2025 - 500 for GET: /test_cgi.pl
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /test-cgi.pl
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /test.py
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /test.sh
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /tmUnblock.cgi
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /uname.cgi
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /viewcvs.cgi
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /welcome
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /whois.cgi
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /
V:Fri Nov 14 07:03:31 2025 - Running scan for "docker_registry" plugin
V:Fri Nov 14 07:03:31 2025 - 500 for GET: /v2/_catalog
V:Fri Nov 14 07:03:31 2025 - Running scan for "HTTP Options" plugin
V:Fri Nov 14 07:03:31 2025 - 500 for OPTIONS: *
V:Fri Nov 14 07:03:31 2025 - 500 for OPTIONS: /
V:Fri Nov 14 07:03:31 2025 - 500 for YJHIKPRC: /
V:Fri Nov 14 07:03:31 2025 - 500 for DEBUG: /
V:Fri Nov 14 07:03:31 2025 - 500 for PROPFIND: /
V:Fri Nov 14 07:03:31 2025 - 500 for TRACE: /
V:Fri Nov 14 07:03:31 2025 - 500 for TRACE: /
V:Fri Nov 14 07:03:31 2025 - 500 for TRACK: /
V:Fri Nov 14 07:03:31 2025 - 500 for TRACK: /
V:Fri Nov 14 07:03:31 2025 - Running scan for "Nikto Tests" plugin
+ 623 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2025-11-14 07:03:31 (GMT-5) (17 seconds)
+ 1 host(s) tested
V:Fri Nov 14 07:03:31 2025 + 623 requests made in 17 seconds
(kali㉿kali)-[~]
$