Oracle VM VirtualBox Manager

File Machine Activity Help

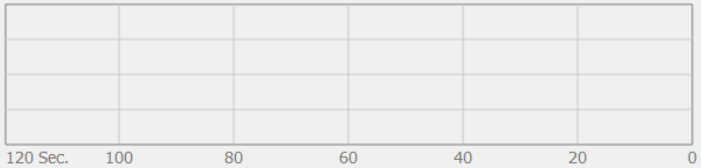
Tools

kali-linux-2023.4-virtualbox-amd64 (Snapshot 1)
Saved

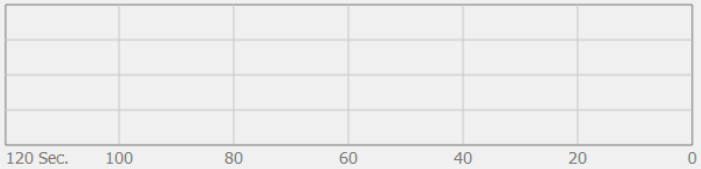
meta2
Saved

Export | Activity Overview | Settings | Discard | Start

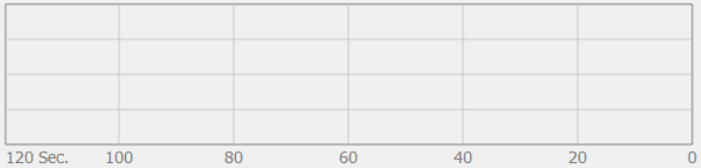
CPU Load
Guest Load: --
VMM Load: --



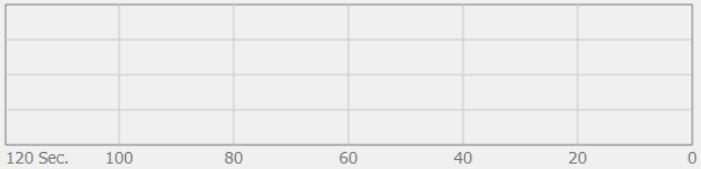
Network Rate
Receive Rate: --
Total Received --
Transmit Rate: --
Total Transmitted --



Disk IO Rate
Write Rate: --
Total Written --
Read Rate: --
Total Read --



VM Exits
Current: --
Total: --



ENG IN
23:07
06-04-2024

root@kali: /home/kali

File Actions Edit View Help

```
ip-https-discover.nse
membase-http-info.nse
riak-http-info.nse

┌──(root㉿kali)-[/home/kali]
└─# sudo nmap --script http-enum.nse -p80 192.168.13.171
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-29 11:59 EDT
Nmap scan report for 192.168.13.171
Host is up (0.044s latency).

PORT   STATE SERVICE
80/tcp open  http
| 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

Nmap done: 1 IP address (1 host up) scanned in 16.55 seconds
```

root@kali: /home/kali

File Actions Edit View Help

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap --script http-grep.nse -p80 192.168.13.171
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-29 12:02 EDT
Nmap scan report for 192.168.13.171
Host is up (0.0022s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-grep:
|   (1) http://192.168.13.171:80/dav/:
|     (1) ip:
|       + 192.168.13.171
|   (1) http://192.168.13.171:80/twiki/TWikiHistory.html:
|     (1) email:
|       + SomeWikiName@somewhere.test
|   (1) http://192.168.13.171:80/twiki/readme.txt:
|     (1) email:
|       + Peter@Thoeny.com
|   (6) http://192.168.13.171:80/twiki/TWikiDocumentation.html:
|     (1) ip:
|       + 08.30.09.28
|     (5) email:
|       + you@yourdomain.com
```

root@kali: /home/kali

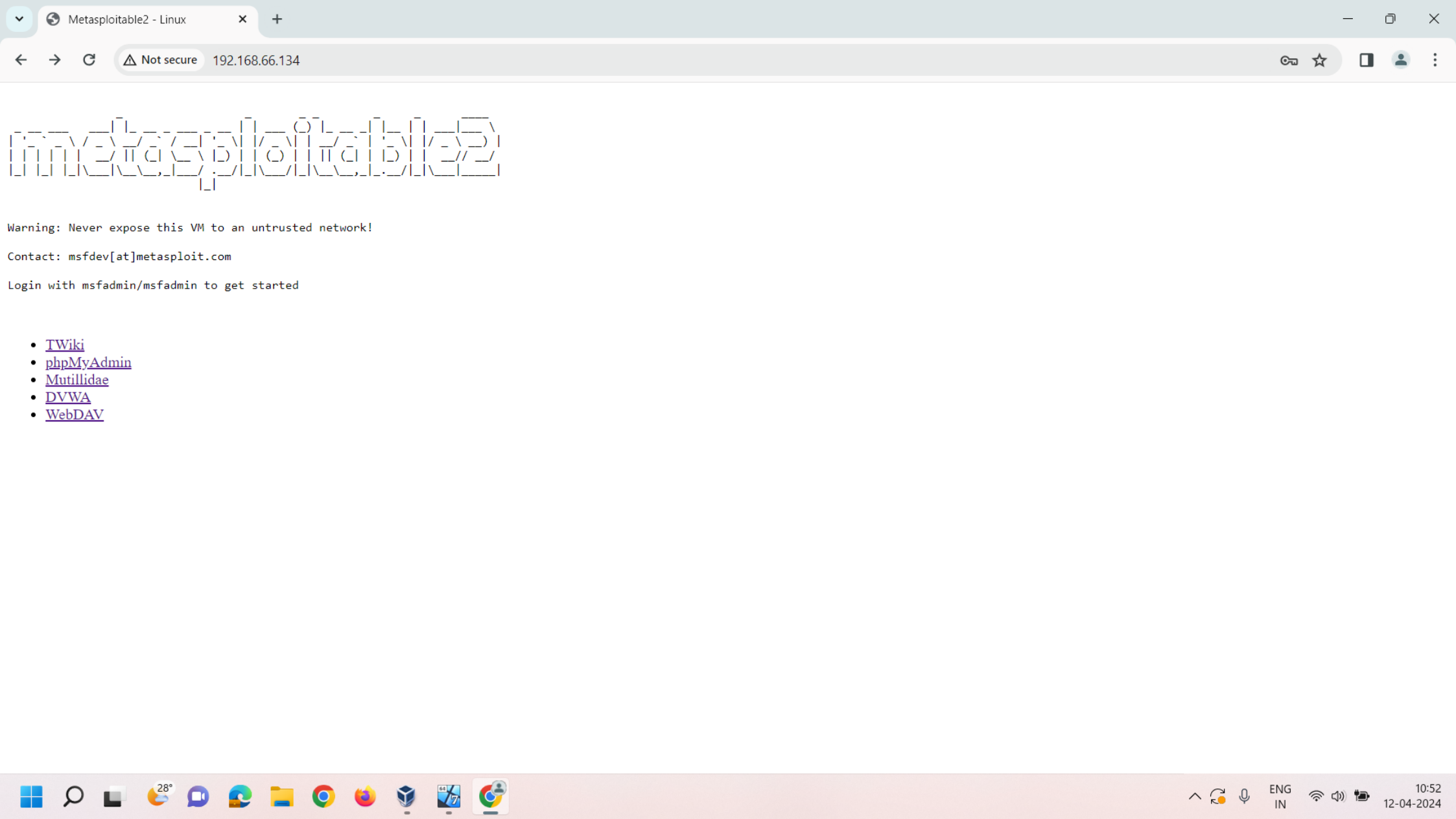
File Actions Edit View Help

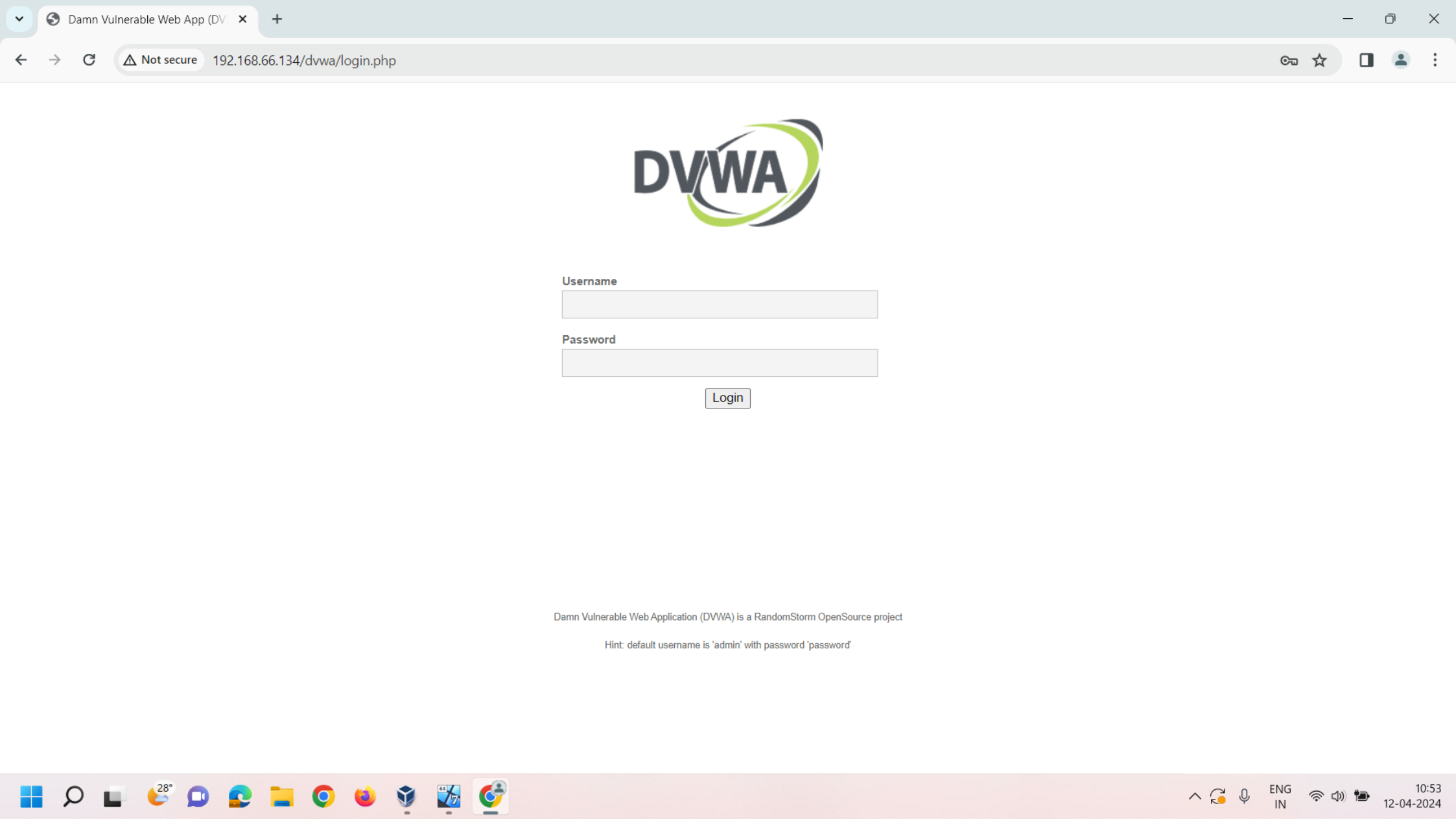
```
Stats: 0:08:57 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Stats: 0:09:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done

┌──(root㉿kali)-[/home/kali]
└─# sudo nmap --script ftp-brute.nse -p21 192.168.13.171 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-29 12:13 EDT
NSE: [ftp-brute] usernames: Time limit 3m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 3m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 3m00s exceeded.
Nmap scan report for 192.168.13.171
Host is up (0.0019s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 1049 guesses in 183 seconds, average tps: 5.4

Nmap done: 1 IP address (1 host up) scanned in 183.43 seconds
```

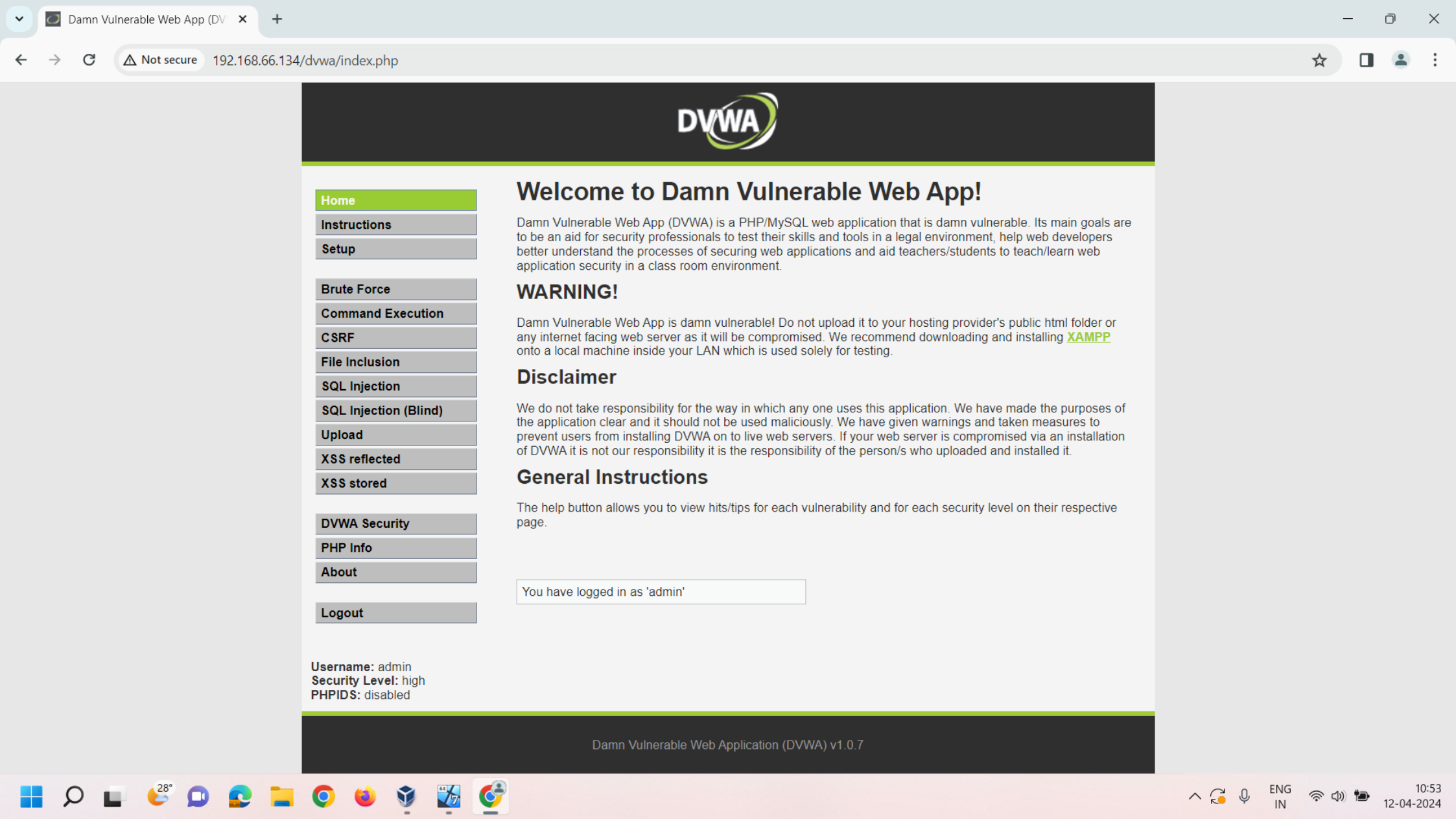
root@kali: /home/kali

File Actions Edit View Help

```
Nmap done: 1 IP address (1 host up) scanned in 183.43 seconds

┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.13.171
Connected to 192.168.13.171.
220 (vsFTPd 2.3.4)
Name (192.168.13.171:kali): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp>
ftp> exit
ftp: lostpeer due to signal 13

┌──(root㉿kali)-[/home/kali]
└─#

┌──(root㉿kali)-[/home/kali]
└─# sudo nmap --script ftp-brute.nse -p21 192.168.13.171
```


Metasploitable2 - Linux
Not secure
192.168.66.134
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
ENG
IN
10:52
12-04-2024


Damn Vulnerable Web App (DV
Not secure
192.168.66.134/dvwa/login.php
DVWA
Username
Password
Login
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'
28°
ENG
IN
10:53
12-04-2024


Damn Vulnerable Web App (DV
Not secure
192.168.66.134/dvwa/index.php
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Welcome to Damn Vulnerable Web App!
Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.
WARNING!
Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.
Disclaimer
We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
General Instructions
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.
You have logged in as 'admin'
Username: admin
Security Level: high
PHPIDS: disabled
Damn Vulnerable Web Application (DVWA) v1.0.7
ENG
IN
10:53
12-04-2024

Welcome to TWiki

- readme.txt
- license.txt
- TWikiDocumentation.html
- TWikiHistory.html
- Lets get started with this web based collaboration platform

TWiki > Main > **WebHome**

TWiki webs:
Main | TWiki | Know | Sandbox

Main . { Users | Groups | Offices | Changes | Index | Search | Go [ ] }

WelcomeGuest: TWiki is a flexible, powerful, secure, yet simple web-based collaboration platform. Use TWiki to run a project development space, a document management system, a knowledge base or any other groupware tool on either on an intranet or on the Internet. You can edit any TWiki page.

The TWiki TM home is at http://TWiki.org/

TWiki Site Map		Use to...
TWiki.Main	Welcome to TWiki... Users, Groups, Offices - tour this expandable virtual workspace. { Changes | Search | Prefs }	...get a first-hand feel for TWiki possibilities.
TWiki.TWiki	Welcome, Registration, and other StartingPoints: TWiki history & Wiki style; All the docs... { Changes | Search | Prefs }	...discover TWiki details, and how to start your own site.
TWiki.Know	Knowledge base set-up - Add TWikiForms for organizing and classifying content. { Changes | Search | Prefs }	...try free-form collaboration, with structure!
TWiki.Sandbox	Sandbox test area with all features enabled. { Changes | Search | Prefs }	...experiment in an unrestricted hands-on web.
You can use color coding by web for identification and reference. This table is updated automatically based on WebPreferences settings of the individual webs. Contact webmaster@your.company if you need a separate collaboration web for your team.		

TWiki.Main Web:

- **TWikiUsers:** List of users of this TWiki web.
- TWikiGroups: List of groups.
- OfficeLocations: Corporate offices.

- [ ] Search (More options in WebSearch)
- WebChanges: Display recent changes to the Main web
- WebIndex: List all Main topics in alphabetical order. See also the faster WebTopicList
- WebNotify: Subscribe to an e-mail alert sent when something changes in the Main web
- WebStatistics: View access statistics of the Main web
- WebPreferences: Preferences of the Main web (TWikiPreferences has site-wide preferences)

TWiki.TWiki Web:

- **WelcomeGuest:** Look here first to get you rolling on TWiki.
- TWikiSite: Explains what a TWiki site is.
- TWikiRegistration: Create your account in order to edit topics.
- Documentation:
  - TWikiFAQ has a list of frequently asked questions.
  - TWikiDocumentation is the implementation documentation of TWiki.
  - TWikiHistory shows TWiki's implementation history.
- How to edit text:

Index of /dav

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.66.134 Port 80