Practical No. 3

Aim: Practical on vulnerability scanning and assessment.

Lab Objectives:

Perform vulnerability analysis using Nikto.

Lab Environment:

1. Administrator privileges

2. Web browser with Internet connection

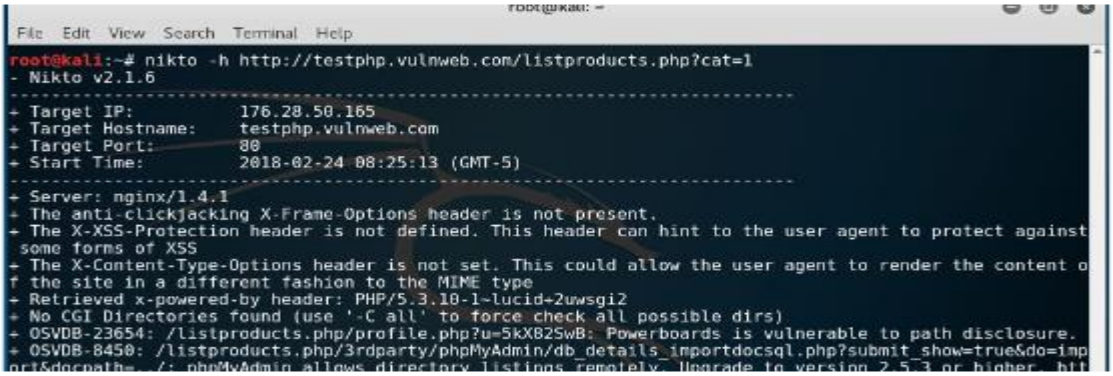
3. Kali Linux

Implementation:

To setup kali Linux for vulnerability scanning and use Nikto to scan for known vulnerabilities, perform the following steps.

1. Log in to kali Linux and open Terminal

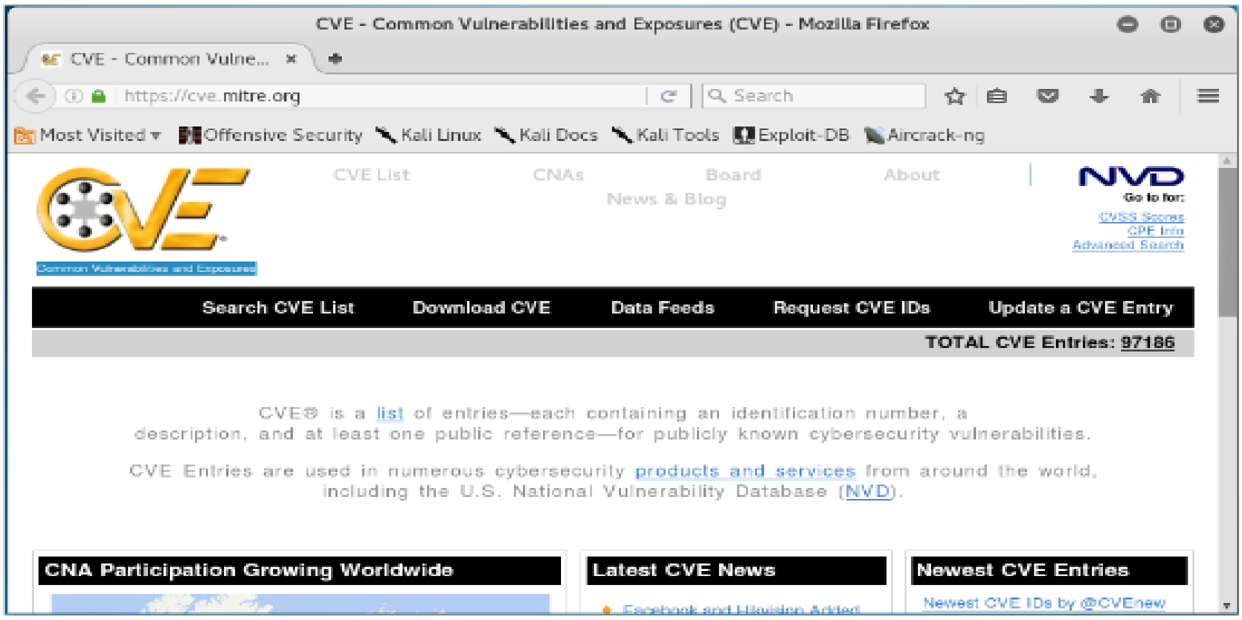
2. Type the command nikto-h <URL of website you want to scan> and press Enter, as shown in figure



```
root@kali:~# nikto -h http://testphp.vulnweb.com/listproducts.php?cat=1
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          176.28.50.165
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2018-02-24 08:25:13 (GMT-5)
---------------------------------------------------------------------------
+ Server: nginx/1.4.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
 some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
f the site in a different fashion to the MIME type
+ Retrieved x-powered-by header: PHP/5.3.10-1~lucid+2uwsgi2
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-23654: /listproducts.php/profile.php?u=5kXB2SwB: Powerboards is vulnerable to path disclosure.
+ OSVDB-8450: /listproducts.php/3rdparty/phpMyAdmin/db_details_importdocsql.php?submit_show=true&do=imp
ort&docpath=../: phpMyAdmin allows directory listings remotely. Upgrade to version 2.5.3 or higher. htt
```

3. Note a vulnerability number, for example 23654, and open a web browser

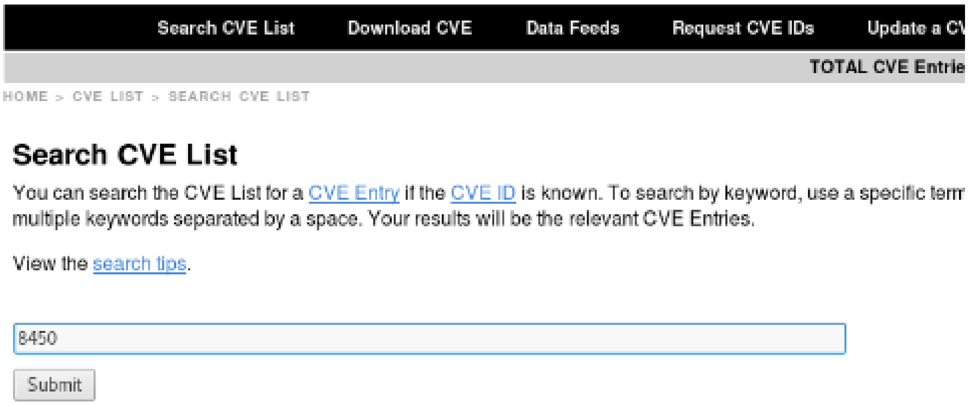
4. Type the URL https://cve.mitre.org/ in the browser to open the common Vulnerabilities and Exposures websites, as shown in figure.



CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.

CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).

5. Click on Search CVE List and type your vulnerability number in the text box, as shown in figure and press enter.



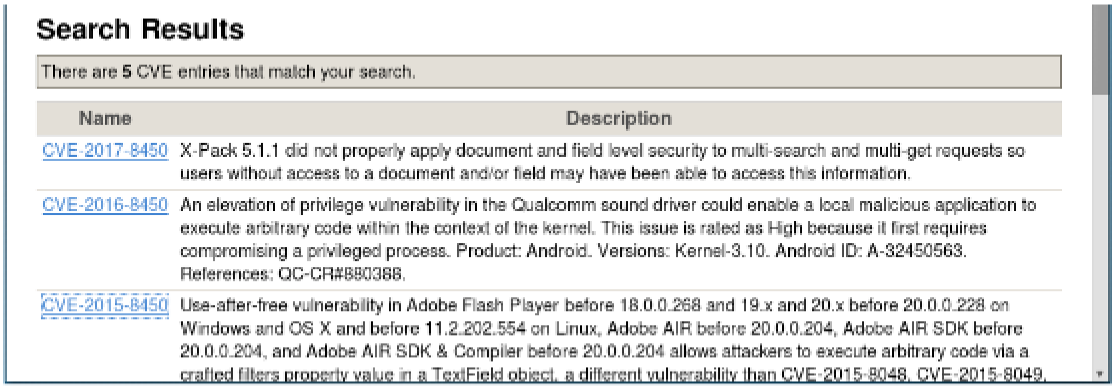
Search CVE List

You can search the CVE List for a CVE Entry if the CVE ID is known. To search by keyword, use a specific terr multiple keywords separated by a space. Your results will be the relevant CVE Entries.

View the search tips.

8450

It will give a list of vulnerability details, as shown in figure.



Search Results

There are **5** CVE entries that match your search.

Name	Description
CVE-2017-8450	X-Pack 5.1.1 did not properly apply document and field level security to multi-search and multi-get requests so users without access to a document and/or field may have been able to access this information.
CVE-2016-8450	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-32450563. References: QC-CR#880388.
CVE-2015-8450	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted filters property value in a TextField object, a different vulnerability than CVE-2015-8048, CVE-2015-8049,