JGI JAIN DEEMED-TO-BE UNIVERSITY | SCHOOL OF COMPUTER SCIENCE AND IT

PROJECT REPORT ON

"WEB APPLICATION PENETRATION TESTING"

SUBMITTED BY

Isaac John Toppo	**18BCAR2018**
Raina Farooq	**18BCAR4015**
Abdeali Aliasgar Waseef	**18BCAR4001**

UNDER THE GUIDANCE OF

Prof. Apoorva K A
Dept of BCA
JAIN UNIVERSITY

ACKNOWLEDGEMENT

Presentation, inspiration and motivation have always played a key role in the success of any venture.

We express our sincere thanks to Dr. B.A Vasu, Center Head, Dr. M.N Nachappa, Head, School of computer science & IT, Jain university, Bangalore for their interest and motivation towards the completion of this project.

We are extremely grateful to our guide, Prof. Apoorva K A, Department of BCA, Jain university, for her guidance and constant supervision as well as for providing necessary information regarding this research and also for their support in completing this endeavor.

We would also like to thank our parents, friends and non-teaching Staff for their support in completing this project

ABSTRACT

Mobile and e-commerce applications are tools for accessing the Internet and for buying products and services. These applications are constantly evolving due to the high rate of technological advances being made. This application is built using Gradle, Java and XML with Android Studio. Android simulators can be used for ensuring proper functionality and for compiling the applications.

CONTENTS

INTRODUCTION

The internet has changed many aspects of society, from business to recreation, from culture to communication and technology, as well as shopping and travelling. This new form of communication has provided new ways of doing business with the help of technological development. E-commerce is the new way of shopping and doing business. It has multiple advantages some of which are;

1. Faster buying process
2. Store and product listing
3. Cost reduction
4. Affordable advertising and marketing
5. No reach limitations
6. Flexibility for customers
7. Easier product and price comparison
8. Several payment modes etc.

Technology has allowed companies to promote and sell their products on new markets, overcoming geographical borders as never before. Consumers have access to a wider market of products when they use wireless and internet technologies. Mobile devices with wide access to the Internet have allowed companies to reach consumers in more diverse ways, thus ensuring deep market penetration.

WHAT IS PENETRATION TESTING?

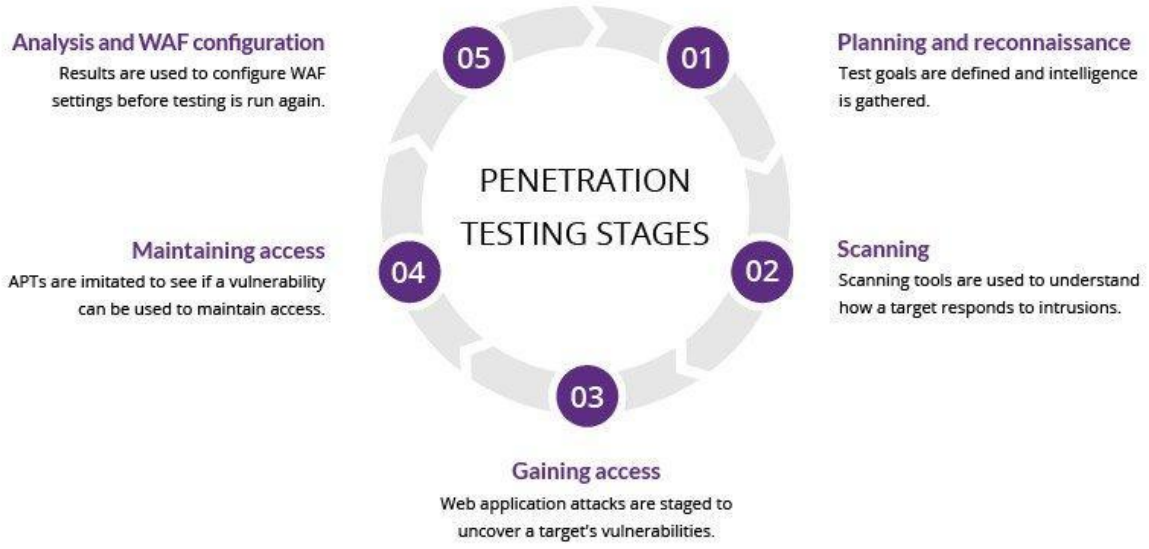
A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall

Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

Insights provided by the penetration test can be used to fine-tune your WAF security policies and patch detected vulnerabilities.

PENETRATION TESTING STAGES

The pen testing process can be broken down into five stages.



1. Planning and reconnaissance

The first stage involves:

- Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.
- Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

2. Scanning

The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:

- Static analysis – Inspecting an application's code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.
- Dynamic analysis – Inspecting an application's code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application's performance.

3. Gaining Access

This stage uses web application attacks, such as cross-site scripting, SQL injections and backdoors, to uncover a target's vulnerabilities. Testers then try

and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

4. Maintaining access

The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent thread, which often remain in a system for months in order to steal an organization's most sensitive data.

5. Analysis

The results of the penetration test are then compiled into a report detailing:

- Specific vulnerabilities that were exploited
- Sensitive data that was accessed
- The amount of time the pen tester was able to remain in the system undetected

This information is analyzed by security personnel to help configure an enterprise's WAF settings and other application security solutions to patch vulnerabilities and protect against future attacks.

PENETRATION TESTING METHODS

External testing

External penetration tests target the assets of a company that are visible on the internet, e.g., the web application itself, the company website, and email and domain name servers (DNS). The goal is to gain access and extract valuable data.

Internal testing

In an internal test, a tester with access to an application behind its firewall simulates an attack by a malicious insider. This isn't necessarily simulating a rogue employee. A common starting scenario can be an employee whose credentials were stolen due to a phishing attack.

Blind testing

In a blind test, a tester is only given the name of the enterprise that's being targeted. This gives security personnel a real-time look into how an actual application assault would take place.

Double-blind testing

In a double blind test, security personnel have no prior knowledge of the simulated attack. As in the real world, they won't have any time to shore up their defenses before an attempted breach.

Targeted testing

In this scenario, both the tester and security personnel work together and keep each other appraised of their movements. This is a valuable training exercise that provides a security team with real-time feedback from a hacker's point of view.

How Does a Penetration Test Work?

Penetration tests can work in different ways—there is no one comprehensive testing method that everyone uses. Part of this is because cyber threats are continuously evolving and pen tests need to simulate whatever attack methods the organization is likely to encounter.

Some of the “broad strokes” of a penetration test include:

1. Assigning a person or team to act as “white hat” hacker(s) to conduct the test at a randomized date and time.

2. Vulnerability management team members scanning the IP addresses of different assets on the network to identify assets using services or operating systems with known vulnerabilities.

3. The penetration testing team conducting a series of simulated attacks against the network using different attack methods. These attacks may target known vulnerabilities from the preliminary scan.
4. The organization attempting to contain, stop and investigating the attack as if it were a real one (depending on how the attack is conducted, the cybersecurity team may not know it is a pen test instead of a real attack).

Types of Penetration Tests

There are several different types of penetration tests used to evaluate the overall security of a network. Here are a few of the most common forms of penetration testing:

1. **Social Engineering Test:** These tests attempt to make an employee reveal secure information, such as a password or a piece of sensitive data. They can be conducted by phone or through online communication and help to identify human-related security vulnerabilities.
2. **Network Services Test:** This common test identifies openings in a network to determine where hackers may be able to gain access into a system.
3. **Web Application Test:** An automated test that determines whether or not web applications and software programs running in the network environment contain security vulnerabilities.
4. **Physical Penetration Test:** A brute force test that seeks to gain access through every physical network device and access point within a facility. This form of test is usually required for military and government organizations.
5. **Wireless Security Test:** This test identifies open or unauthorized hotspots and WiFi access points and attempts to gain network access through them.
6. **Remote Dial-Up Test:** Modems represent a potential weak point in a network. This test searches for modems in a network environment and tries to log into them using brute force methods to gain system access

Why Is Penetration Testing Important?

In 2015, Ponemon Institute conducted a study on the cost of data breaches that surveyed 350 organizations from 11 different countries that had suffered data breaches. Nearly half of said breaches (47%) were the result of a malicious attack and the rest happened because of system glitches and human errors

As companies are digitizing their business operations and processes, we tend to underestimate the new technology risks we are exposed to. One of the major risks is hackers exploiting a vulnerability that exists within your IT infrastructure. The possibility that the hacker could take full control of your IT infrastructure becomes extremely likely once they gain entry into your internal network.

The main reason penetration tests are crucial to an organization's security is that they help personnel learn how to handle any type of break-in from a malicious entity. Pen tests serve as a way to examine whether an organization's security policies are genuinely effective. They serve as a type of fire drill for organizations.

Penetration tests can also provide solutions that will help organizations to not only prevent and detect attackers but also to expel such an intruder from their system in an efficient way.

AGENDA

Creating a website project that teaches people how to “hack” Itself with interactive guide and an easy setup process that is Similar, and which is also easy to understand . Goal is to create a finished product and platform for learning security

Use Case

The Website can be used in the field of education to kickstart the learning process by downloading the files provided. We have learning modules that are for people who don’t have access to Computer labs or High-end Systems to Run Vms just experience something as simple as Linux.

The Guides Provided are Easy and Well illustrated for Beginners and will be provided at the end of the Research Document.

This Project can be utilized in Awareness Programs for Cyber Security or can be utilized to Benchmark Vulnerability Scanner Software.

Since The Project is Open Source it will also me used for Design Reference and can be user to reuse Many of the UI Features for Other Projects, The Code Written is Easy to understand with modern UI features will have the ability to mark as reference for people studying the subjects

INITIAL STUDY

To find Barriers and difficulties in learning computer science we will refer to different studies that may direct the project to mitigate at least one of the issue that plagues the aspirants to enter the industry

Study I

To Review the Barriers of Ict Application in Payam Noor University of Mazandaran from Professors and Student Point of View

Sample sizes were selected according to scientific principles and sample size tables of 247 professors and 381 students as well as multi stage cluster sampling methods of the mentioned population. The research method is survey-based and the questionnaire was used to analyse the questions related to the survey. Therefore the questionnaire contained 21 questions which include five components: cultural barriers,human barriers, technical and physical barriers and financial barriers and also comparison between these barriers.to review the barriers of ICT usage,professors and students point of view were considered.

-----By Samire mortazavikiasari

Link :
https://www.sciencedirect.com/science/article/pii/S1877042812023713

We find that human interaction and financial barriers are the biggest factor in limiting the ease of
learning computer Science (ICT) as concluded by the study from the survey taken below

Distribution of impact from teachers' point of view	Distribution of impact from students' point of view	Micro-scale	Variable
%21	%50	Weakness of acceptable definition among ICT users	Cultural variable
%4	%3	Weakness of electronic teaching and learning	
%2	%18	Weakness of individual ownership law	
%8	%9	Traditional operation of educational system	
%5	%5	Dominance of hardware view over software one	
%57	%4	Presence of a view indicating the use of ICT as a way of dissoluteness, depravity and corruption	
%3	%11	Presence of various decision-making institutions with respect to ICT use	
%12	%7	Users' weakness in knowing English	Human variable
%5	%46	Traditional performance of modern methods in the class	
%57	%13	Lack of an appropriate teaching about using ICT	
%19	%28	Users' uncertainty of accessibility to required information	
%9	%8	Lack of adequate motivation for using ICT	
%13	%13	Low IC accessibility speed	Technical-skeletal variable
%56	%49	Communication network cut-off as users are using ICT	
%20	%27	Lack of national policy on the use of ICT	
%11	%11	Lack of internal harmony among related organizations	
%12	%7	Lack of congruency between educational facilities and the number of users	Financial variable
%6	%51	Weakness of supporting organizations to support communication networks	
%56	%11	Absence of proper investment in communication network development	
%18	%6	Absence of allocation of proper time to use ICT	
%8	%25	Lack of appropriate motivating tool of using ICT	

Distribution of each effective barrier to use ICT (Technology of Information and Communication) from the teachers' and students' point of view based on regression equation.

Financial variable	Technical-skeletal variable	Human variable	Cultural variable	Sample group
%23	%11	%59	%7	**Students**
%26	%47	%18	%9	**Teachers**

According to above table, the maximum proportion was human factor with 59% among all other effective factors being studied with respect to the use of ICT from students' point of view followed by financial factor with 23%, technical - skeletal factor with 11% and cultural factor with 7% respectively.

Our conclusions from the study are in line with this paper. Thus the observations made helps us understand this subject more

“ Based on data analysis, the maximum proportion of influential factors was a consequence of human resource with 59% followed by financial factor with 23%,technical skeletal factors with 11% and cultural factor . University teachers had different ideas as they stressed the technical-skeletal factor as the highest proportion with 47%.
They then considered financial factor with 26%, human factor with 18% and cultural factor with 9% as subsequent proportions which were similar with the percentage that students assigned to three subsequent factors of using ICT. “
Observation : in both the teachers and student Views Financial barriers are the second
most priority to overcome, with the first most priority varying from technology
infrastructure for teachers and human resources for the students.
Note: the study was conducted in IRAN and in contrast to INDIA, Iran’s integration of modern
technologies in their infrastructure can be seen as similar to indias as both face similar issues of
ICT education due to language ,and cultural barriers.
Study II

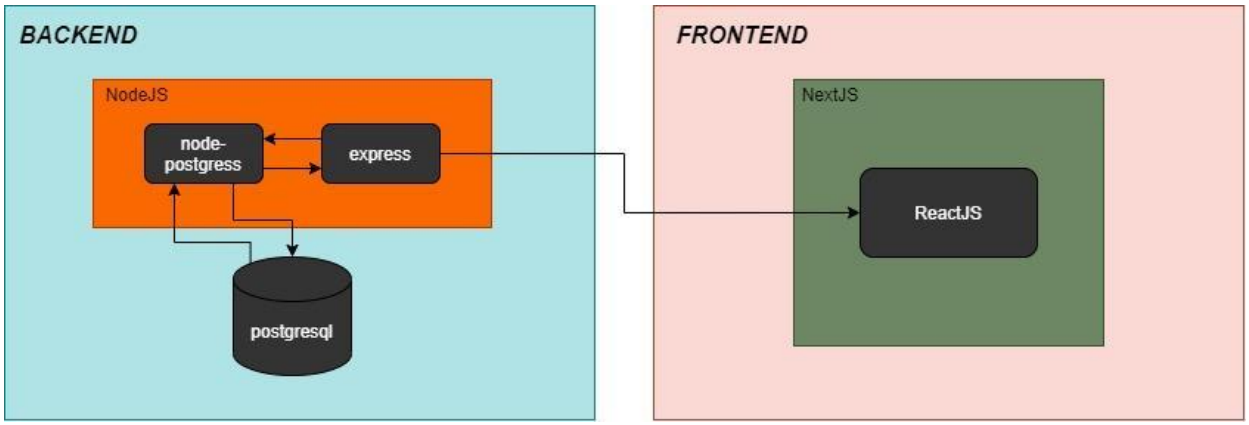
Computer Science Education Research – An overview and some proposals

Anabela de Jesus Gomes
Coimbra Institute of Engineering, Coimbra-Portugal
Centre for Informatics and Systems, University of Coimbra-Portugal
António José Mendes
Centre for Informatics and Systems, University of Coimbra-Portugal
Maria José Marcelino
Centre for Informatics and Systems, University of Coimbra-Portuga

It is known that many students encounter a lot of difficulties in introductory programming courses. Possible reasons for these difficulties are discussed and some existing proposals in the literature are presented.

The solutions proposed by this paper talks about providing visuals aid and giving creative freedom to students to choose their activity helps in better retention and motivation to pursue the subject and have seen less dropouts with volunteers

SYSTEM ARCHITECTURE



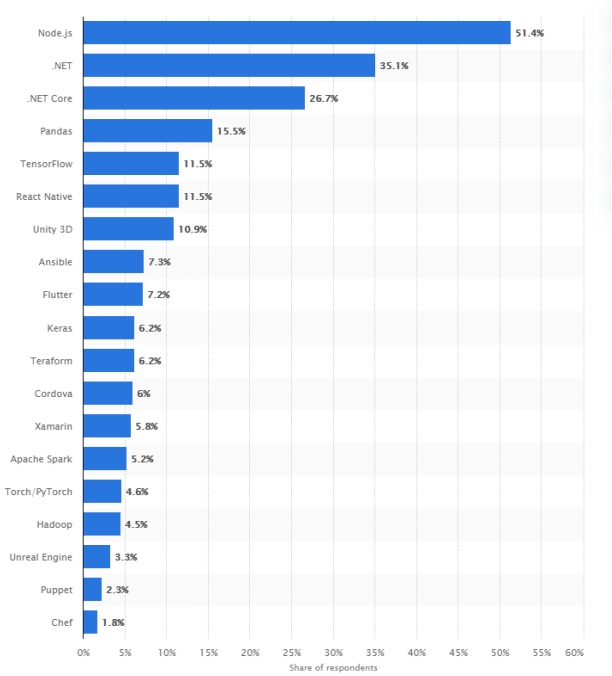
The project aims to represent latest trends in web technology hence it uses technologies which are being used most in today's climate. Below we will discuss the technologies used and the reason they're being used in this project.

Backend:

1. NodeJS:

   NodeJS serves as the backend of the project as it is one of the most preferred framework as of 2020 for new developers.

   (Image source:



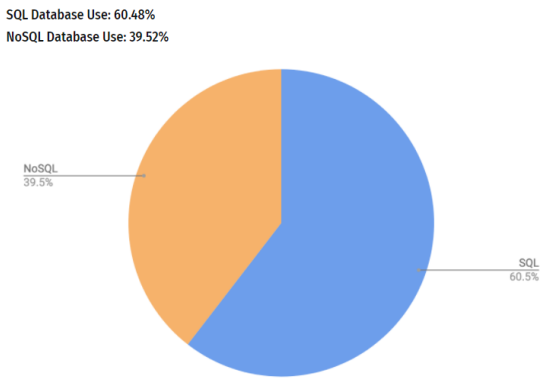
https://www.statista.com/statistics/793840/worldwide-developer-survey-most-used-frameworks/)

Another reason NodeJS was selected was due to the way it ties up to the rest of the architecture of our web app. It has clean integration with postgresql database which is our preferred database (reasons explained below) using the node-postgress npm-package. And its also based upon the same language i.e Javascript as our front-end which makes development much smoother.

2. Express
   We are using express in NodeJS to create a HTTP server for our API endpoints. Express has been called the de facto standard server framework for Nodejs due to its simplicity and its flexibility.

3. Postgresql
   Postgresql is used as our database of choice as it is the more commonly used relational database in current times in combination with Nodejs. It is also Open Source which attracts a lot of new developers to use it in their projects.

   The reason of going with a SQL database instead of a more trending NoSQL database is that a SQL database represents the current share of technologies on the internet more than NoSQL. While NoSQL is gaining popularity fast it still has a long way to go before majority of websites on the internet use it instead of a more traditional SQL relational database.



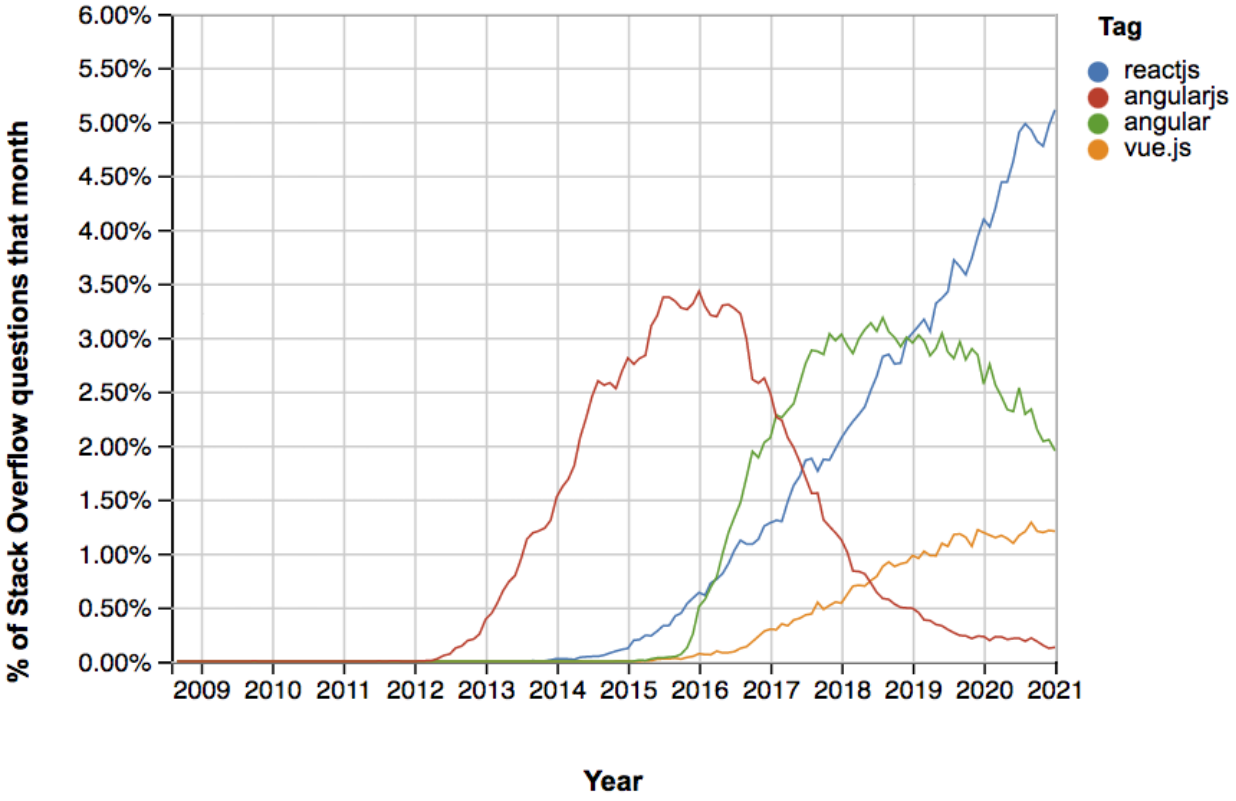
(Image source:

https://www.statista.com/statistics/793840/worldwide-developer-survey-most-used-frameworks/)

FRONTEND:

1. NextJS
   Next.js is an open-source React front-end development web framework that enables functionality such as server-side rendering and generating static websites for React based web applications. There is an increasing trend of using NextJS instead of just ReactJS because it provides SSR (hence better Performance), SEO and a complete Routing System. This results in a lot of new businesses choosing NextJS as their preferred Frontend Framework.

2. ReactJS
   NextJS uses ReactJS under the hood. React is an open-source, front end, JavaScript library for building user interfaces or UI components. It is maintained by Facebook and a community of individual developers and companies.



Source: https://insights.stackoverflow.com/trends?tags=reactjs%2Cvue.js%2Cangular%2Cangularjs

ReactJS has taken its place in the web development market and currently stands unrivaled. This gives us all reason to build our web app around it as practicing penetration testing on a React website gives a similar experience to performing a pen-test on majority of websites created in recent years.

UI design

Information design

Information design is a process that prioritizes the final goal or outcome of the project and builds a system that produces a reaction based on how the information is layered to the viewers. This is used in many industries such as News, Ads, Entertainment, activists movements, social media, education and many more, where all of them can provide the same information but can receive different reactions based on the presentation. Example: to spread Covid 19 awareness among people news social media can receive LOLs and 😂😂 for the meme whereas Ads can get a response in increase sales but on the other hand news may receive debates and discussions. Despite the information being the same such as wearing a mask or not going outside, we need to first prioritize the goal of the project and see what kind of reaction we are looking for.

Goal of design

We are looking for the response of “ that’s so easy ”. Why? We want to make cyber security not only Accessible but first and foremost beginner friendly which then demands the project to be more

- Engaging
- Have Pictorial representation.
- Must be intuitive
- Clear separation of components
- Looks professional
- Has a user feedback to every action

What does all this mean?

Well it simply means that any person who may interact with any element or asset from WAP will be able to feel comfortable in exploring and will stay engaged and to do so we will use modern design techniques to catch attention and increase attention span for the viewers.

Guide doc design.

The guides are specially made for beginners and are pictorially represented with less text and more illustration elements to guide the eyes of the reader to follow a path in the text unconsciously making it more comfortable for the mind to go through the documents. Every page has different font types, illustration, background colour all for a purpose.

For fonts the most new research has been in relation to the physical characteristics of text. Font type, spacing and proportionality of lettering have been growing areas of focus. And all are shown to affect recall of information. Most recently, Princeton University (of which the RMIT research was based) attempted to understand if harder to read fonts really do help us remember things. And it appears that they do. Thus to increase attention span and capture the eyes to different topics, different fonts and it's sizes are used.

Link – https://psycnet.apa.org/record/2005-06924-003

Journal of Educational Psychology published results of a study that show in less than 24 hours the advantage of more text disappears. Indicating that it really is about quality and not quantity when it comes to better

performance. Thus less write-up and more Pictorial representation may improve engagement

🔗- http://faculty.washington.edu/chudler/font.html

All these techniques will ensure user engagement and beginner's friendliness for wap project with its guide style

Website design – UI

The home page

Its jet the effect of glass UI which was a trend in early 2021 and color Auroras which was also a trend in late 2020 all of it is done in css with **blur, opacity and keyframes** to hey the effect.

There is parallax effect and flex box for a gift and paragraph

Exercise page

Uses same effect as home page but have inverse values

Download page

Display is set at block so all download containers are stacked on each other where on left there is info and download button and on right there is an illustration

About us page

It has a custom gradient background with circular waves, it is not an image but a simple css trick along with cards that present our pictures, name and a quote from us.

Linux Online

This one is a lil special because it uses JavaScript. RiscV emulator that runs Linux. To the right you may find a document , but not any ordinary documents as it auto highlights the keywords as you scroll down making it easy to divert the eyes of the user to minimal and crucial information in your document

Framework

Next. Js is a react. Js framework that divides all the elements to components which is like having oops In C++, how do you ask? Well, components that have things like div and h1 will be called and changed only if they are updated or manipulated by the user but it doesn't re-render the entire page.

In simple words if you had time displayed in your blog website , the entire blog doesn't have to refresh and load up whenever a second passes and the time value has to be updated. In React only the time component refreshes making websites made with reach much faster

Implementation of react

You can see the most obvious one being the Navigation Bar, where it doesn't need to load itself again and again, whenever we change pages. React also unloads any js that's not being used making heavy application very light

We can also see this different of speed in another experimental website https://bitsoffiber.netlify.app/

Another project that is made with simple html, css, js but is very slow compared to this project due to the simple reason that in the old method all the js is loaded , even the unused one and this could be js code for opening a page but since it’s never used it eats up space and processing power

Next js

Strictly speaking of UI design the one change you will see is that css filé need to be saved as `name.module.css` and there are no html files as everything is written in JSX . File structure and routing of pages, js modules is more organized especially when collaborating with other developers

Collaboration and Coding

Collaborating with other people for coding projects demands a lot of organization, labeling, and communication between developers. During the project, we had to divide the work based on our strengths but also push our skills and become professionals. Labeling and organizing file structures to avoid accidental deletion of work was the worst-case scenario which fortunately never happened in our project. plus everyone was keeping copies or backup of the work regularly.

Github

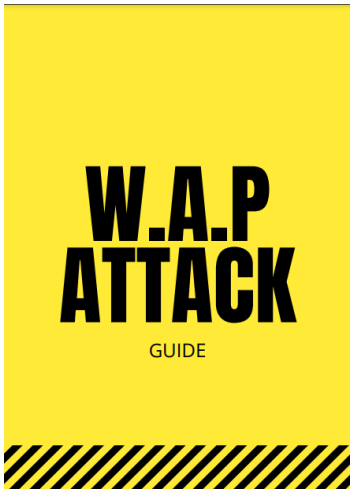
It was the most useful tool due to its versatility. it made collaboration on the project easier and with multiple branches, we made sure that nothing that previously worked broke due to someone else input. Github makes it very easy to download and update the source code or a complex web application as we also made descriptive commits to keep track of all the changes we were adding to the website.

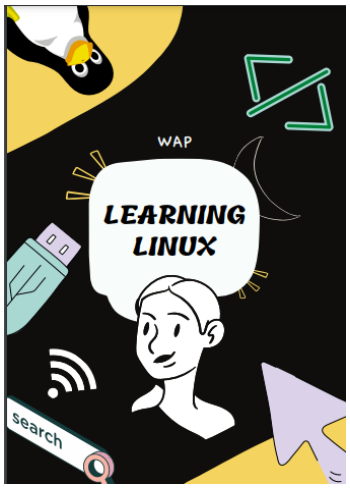
the Branch features and Git clone Features make it open to everyone to make different versions of WAP

Write Up Provided for WAP

Three Documents are provided below that is available to download on the website and is recommended to use the Material provided to understand better about how to use the website

The Documents are for Complete beginners thus are more Poster like and have heavy Visuals





Bibliography

1. **http://faculty.washington.edu/chudler/font.html**
   - Eric H. Chudler, University of Washington

2. **The Influence of Font Type on Information Recall.**
   Gasser, M., Boeke, J., Haffernan, M., & Tan, R. (2005). The Influence of Font Type on Information Recall. North American Journal of Psychology, 7(2), 181–188.

3. **https://insights.stackoverflow.com/survey**

4. **To Review the Barriers of Ict Application in Payam Noor University of Mazandaran from Professors and Student Point of View**
   Samire mortazavi kiasari-

W.A.P ATTACK

GUIDE

CLICK HERE

Welcome to WAP!

Learning made easy for `Web Application and Penitration`

Downloads →

ISO files ,PDF and many other goodies.

Start Learning →

Lets Begin the Hunger Games.

Linux Online →

Getting on with the basics.

About us →

Wanna Know more about us, click here!!

Welcome to WAP!

Learning made easy for `Web Application and Penitration`

XSS Attack →

ISO files ,PDF and many other goodies.

HTML Insertion →

Lets Begin the Hunger Games.

CSRF Attack →

Getting on with the basics.

PassWORD Attacks →

Wanna Know more about us, click here!!

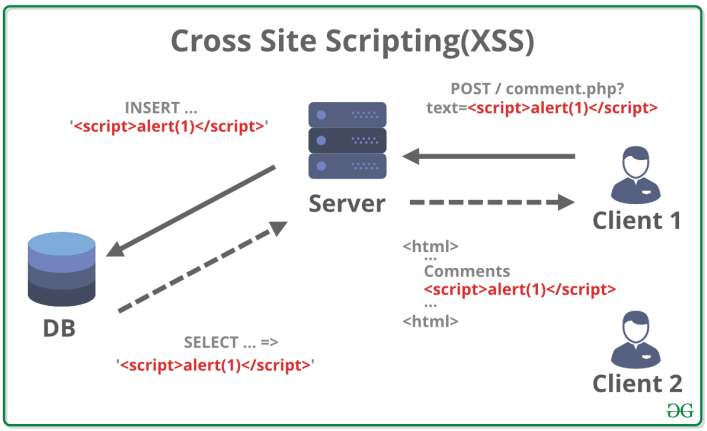
SQL Injection →

Wanna Know more about us, click here!!

XSS attack

EASY THAN YOU THINK

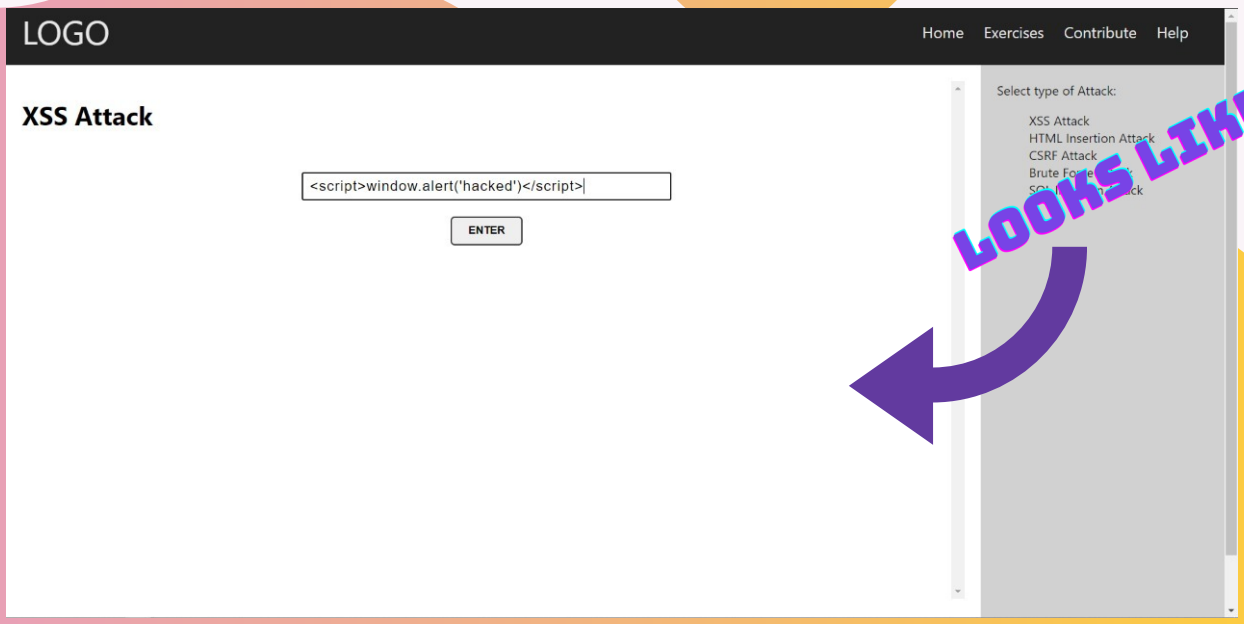
Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.



In general, effectively preventing XSS vulnerabilities is likely to involve a combination of the following measures: Filter input on arrival. At the point where user input is received, filter as strictly as possible based on what is expected or valid input. Encode data on output.

HOW TO?

1.Go to xss attack page



2.Type this command in the search bar and press enter.

```
<script>window.alert('hacked)</script>
```

3.You should see an alert window which means this was successful

HTML

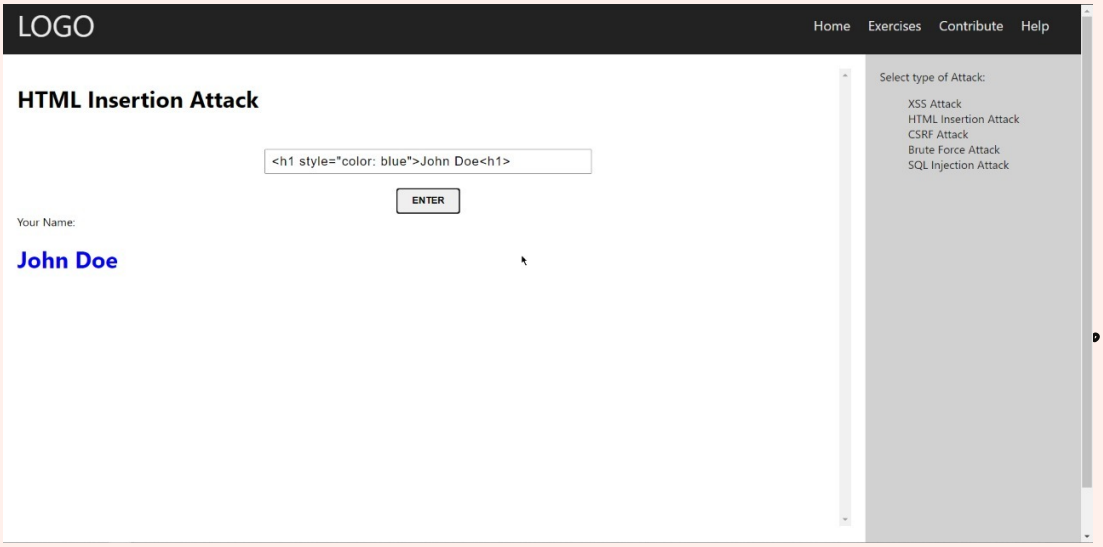
INSERTION ATTACK

HTML injection is a type of injection vulnerability that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page. ... For example, malicious HTML code can be injected via the innerHTML JavaScript method, usually used to render user-inserted HTML code.

The most common way of detecting HTML injection is by looking for HTML elements in the incoming HTTP stream that contains the user input. A naïve validation of user input simply removes any HTML-syntax substrings (like tags and links) from any user-supplied text. To avoid false positives, the security mechanism that detects possible injections and protects the application should learn in what application context user input is allowed to contain HTML. Also, it should be able to stop HTML input if it learns that such text is pasted as-is in web page generated by vulnerable application components.

Instructions

1.Open the HTML insertion attack page



2.Now type the following in the search bar to de-face the website

```
<h1> style="color: blue">your name</h1>
```

3.Did you see your name in blue in the webpage ?

THIS IS

SQL

INJECTION ATTACK

Retrieving hidden data, where you can modify an SQL query to return additional results.

Subverting application logic, where you can change a query to interfere with the application's logic. UNION attacks, where you can retrieve data from different database tables.

Prevention Methods

1. Validate User Inputs.
2. Sanitize Data by Limiting Special Characters.
3. Enforce Prepared Statements and Parameterization.
4. Use Stored Procedures in the Database.
5. Actively Manage Patches and Updates.
6. Raise Virtual or Physical Firewalls.
7. Harden Your OS and Applications.

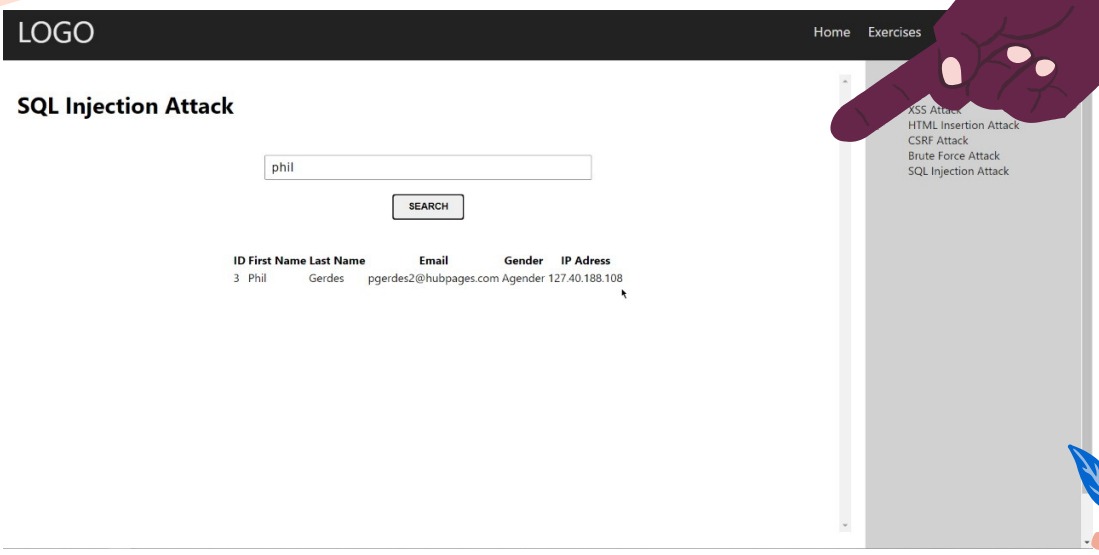
STEPS TO FOLLOW

Beginner friendly

Let do something that is easy and will let us see all the details in the database. when you type in the search bar you should receive a all the information related to the search

1. type the name 'phil' and press search

you should see some results down below . but what if you wanna see other people and the details? Without a valid name its a useless endeavor or is it ?



Okay, now to find all the information we will use sql injection

```
2.type this " ';-- "
```

Press enter and you should see almost all the results in the database as the will be dumped in the webpage

so whats happening?

```
String sql = "SELECT * FROM database WHERE name LIKE '% INPUT %';
```

now this command takes in name and cheackit but lets see what happnes when we add our code

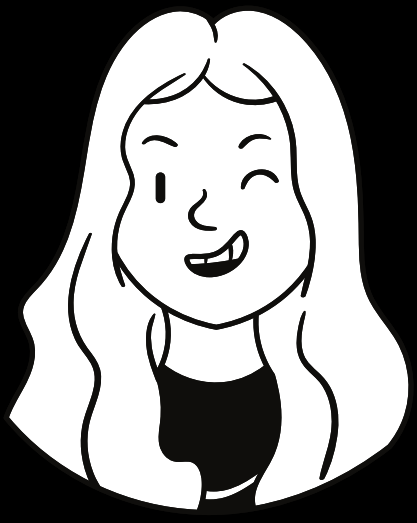
```
String sql = "SELECT * FROM database
WHERE name LIKE'%';-- %';
```

this `;` ends the statement that lets the user to enter another sql command.

FOR OTHER ATTACKS

REFFER TO RESEARCH DOCUMENTATION

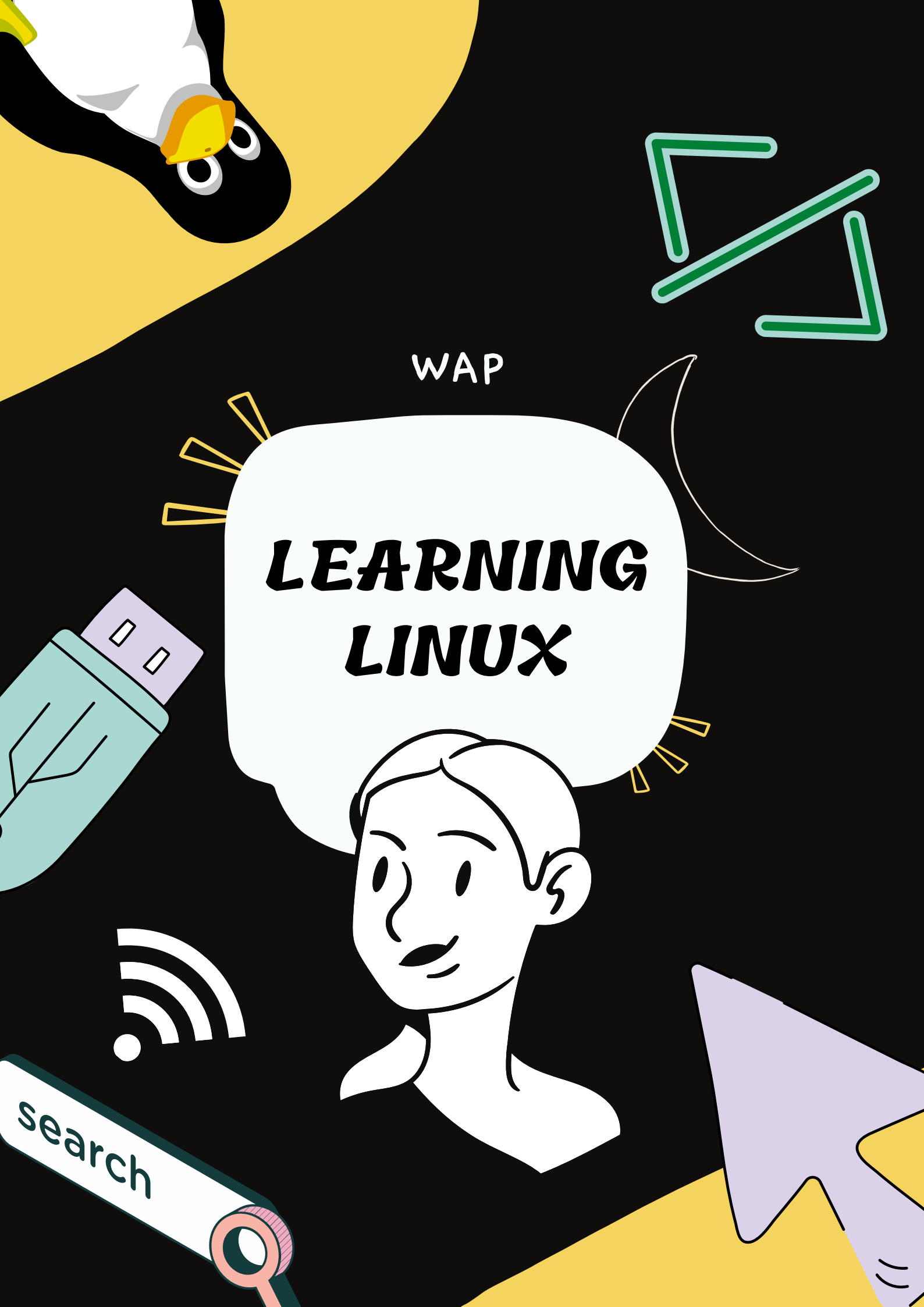
Under sections Exercise



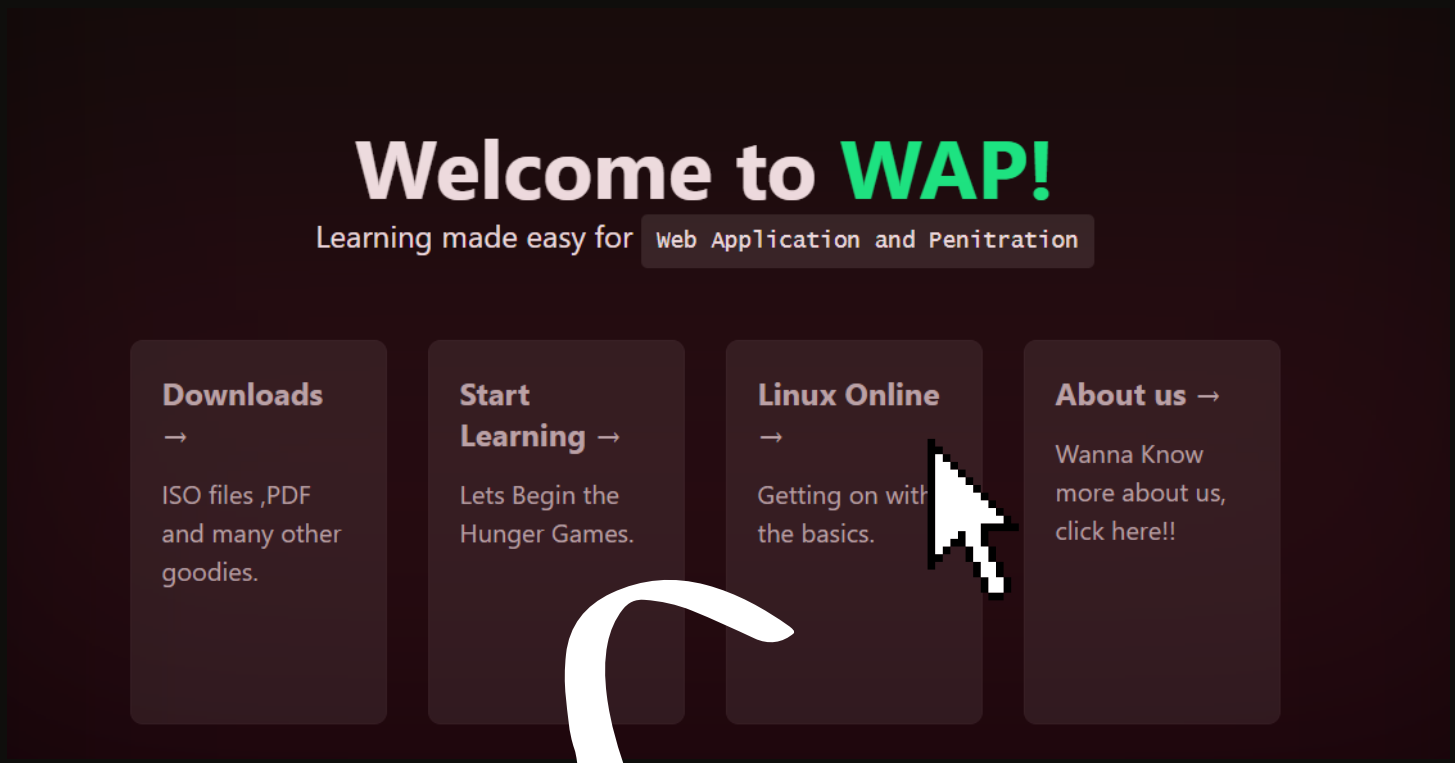
Raina Farooq

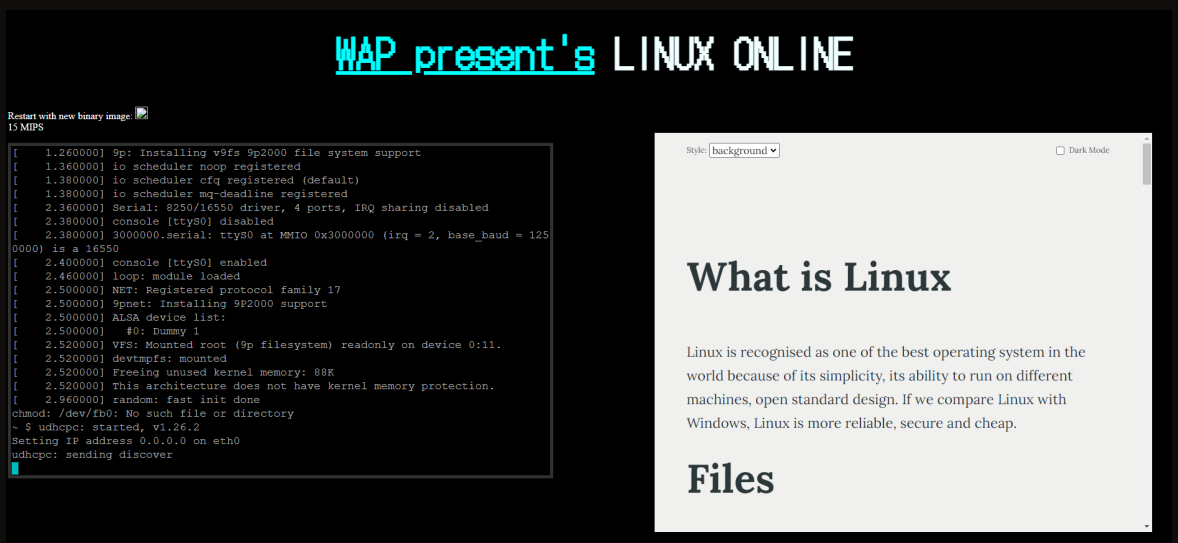
Isaac John Toppo

Abdeali Aliasgar Waseef


WAP
LEARNING
LINUX
search

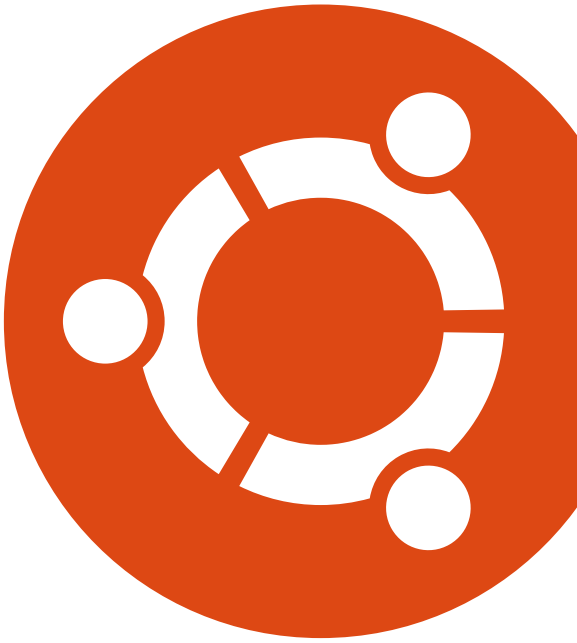
click on 'linux online'





What is Linux

INTRODUCTION



Linux is a reliable, multiuser and secure operating system. Linux implemented the concept of cross platform standardisation, due to which you can find Linux on massive mainframes, on distributed clusters, on PCs, on Apples, on tablets, on smartphones, on wristwatches, in automobiles etc.

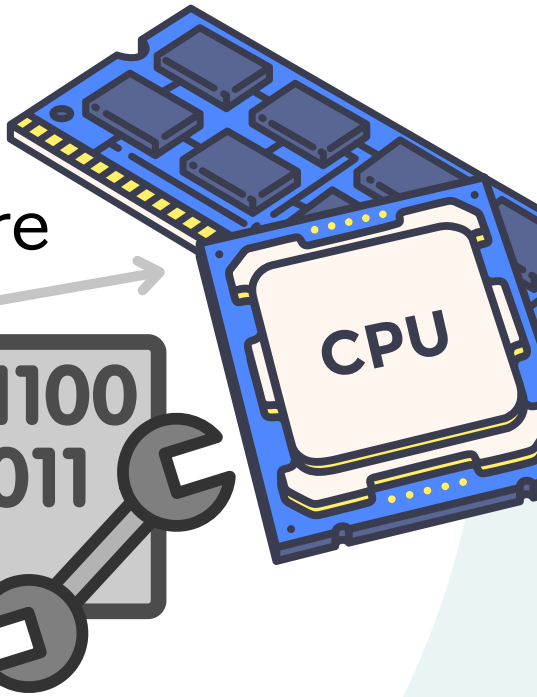
Linux continues to dominate web and application hosting landscape.

While Linux is adored by academicians, Linux has a great commercial domination. Linux is open source unlike other UNIX clones.

Linux is recognised as one of the best operating system in the world because of its simplicity, its ability to run on different machines, open standard design. If we compare Linux with Windows, Linux is more reliable, secure and cheap.

BASIC STRUCTURE OF LINUX

Linux System Architecture



1. Hardware layer
2. Kernel
3. Shell
4. Utilities

Hardware layer

This layer is not part of UNIX operating system. This layer consists of all peripheral devices like RAM, hard disk, CPU.

KERNEL

Kernel is the core component of Operating System where actual code and functionality of operating system lies. The kernel interacts with the hardware layer and provides services to user. If a user program/ application needs to access the hardware, it ask's kernel, which performs the job on user behalf. The user programs access the kernel through a set of functions called system calls.

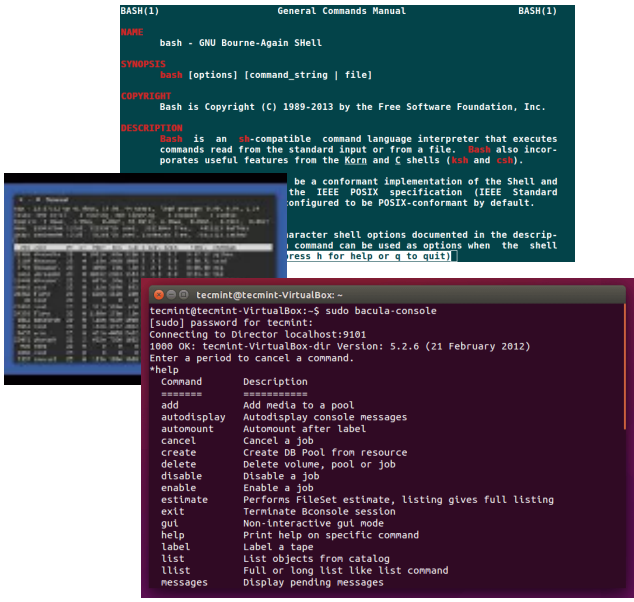
kernel handles the following operations

- Scheduling running of user and other processes.
- Allocating memory.
- Managing the swapping between memory and disk.
- Moving data to and from the peripherals.

It receives service requests from the processes and honours them. All these services are provided by the kernel through a call to a system utility(command shells as we will see later).

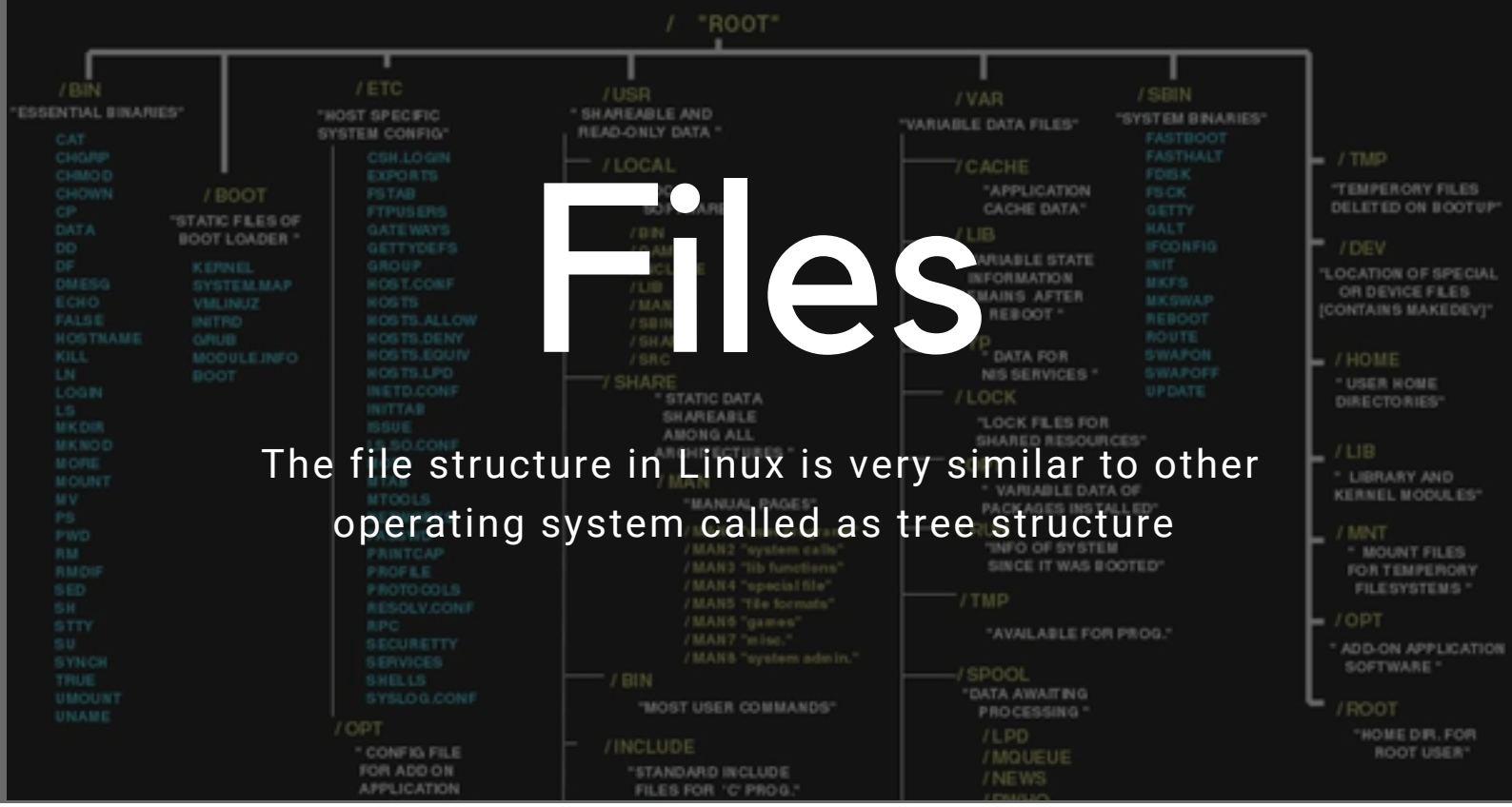
Shell

An interface for the user through which he can interact with the operating system. A shell environment allows you to run commands, programs, and shell scripts.



Utilities

Utility programs are the commands that perform a single task like printing date and time or searching a file in given directory. Different commands can be combined.

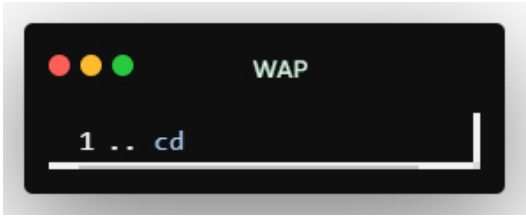


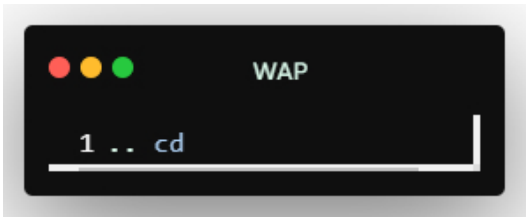
Files

The file structure in Linux is very similar to other operating system called as tree structure

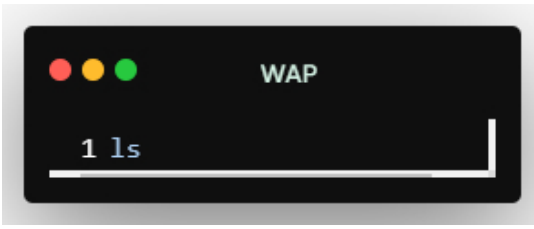
Lets learn about the file structure with some commands.
Follow along the instructions in this lesson

First click on Learn Linux in the Home page and let the page load out
Now for your first command type <..cd> twice

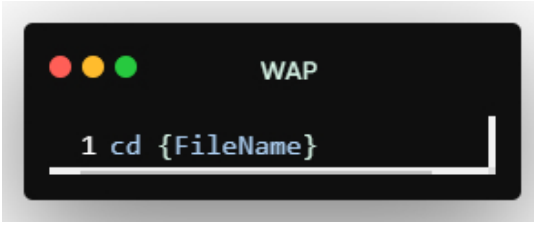




Now to too look at file type



Cool right ?!, these are file of the Linux system and you can go and explore them by using the above commands where ".. cd" is used to go back, and "ls" is used to display or list the files. you can use cd (Enter the filename) to open the files



Clear
This will clean all the clutter above

```
clear
```

WAP

```
1 $ Clear
```

CAT
Refresh the page cuz now we will look how to display files with CAT. The three basic functions of cat are: displaying files, combining copies of them and creating new ones
File Creation

```
cat > filename
```

WAP

```
1 cat > {filename}
```

Displaying Files/Reading Files

```
cat filename
```

WAP

```
1 cat {fileName}
```

Copy Original to copy file

```
cat filecopy >filename
```

WAP

```
1 cat {Original fileName} > {Copy filename}
```

Disk Related command
How do I check free disk space in Linux operating system? UNIX offers two commands for checking out free disk space:
(a) df command Report file system disk space usage.
(b) du command: Estimate file space usage.

WAP

```
1 df
2 df-h // more details
3 du
4 du-sh // space used
```

Vi Editor
To make a txt file
Type the 'vi ' command with a file name like its givin below and then the vi cmd open's up that let you type what you want. After typing press escape and type the next command ':wq'. Now to check type cat filename.

```
1 $ vi {filename}
2
3 ----------------VI-----------------------
4 ~/type some thing her
5 ~/
6 ~/
7 ~/
8 ~/
9 ~/
10 ~/
11 ~/
12 :wq // press Esc and then the CMD to Save and Quit
13 ----------------VI-----------------------
14 $ ls
15 filename
16
17 $ cat filename
18              type some thing here
19 $
```

Bonus cmd!

to check web connection

PING (WEBSITE NAME)

PING 1.1.1.1

Example

WANT TO KNOW MORE ABOUT SYSTEM YOU ARE USING

UNAME

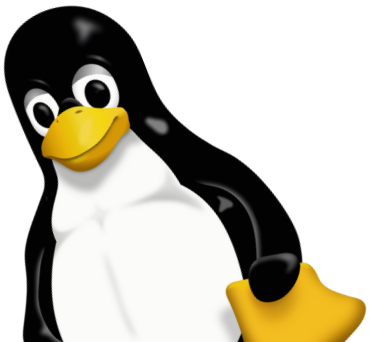
COMMAND FOR SYSTEM INFO

Example

```
uname -s
uname -m
uname -a
```

Manual Setup

WEBSITE SETUP INSTRUCTIONS



IT IS RECOMMENDED TO DOWNLOAD THE VM VERSION OF WAP

Warning !!!!

Open Terminal and update your system with 'apt-get update' then type the following command in the terminal

```
$. sudo apt install node npm postgresql
postgresql-contrib

$. sudo service postgresql start

$. sudo -u postgres psql postgres

$. \password postgres, password, password
$. \q

$. git clone https://github.com/wabdeali/final-
project-frontend

$. git clone https://github.com/wabdeali/final-
project-backend
```

```
$. cd final-project-frontend , npm install

$. cd final-project-backend , npm install

$. (In psql) CREATE DATABASE vulnwebapp;

$. psql -U postgres -h localhost -p 5432
vulnwebapp < vulnwebapp.sql (Execute in /sql
directory in regular terminal)

$. node index (in backend)

$. npm run build (frontend)

$. npm run start (frontend)
```

AND ITS DONE

Open the link in the terminal