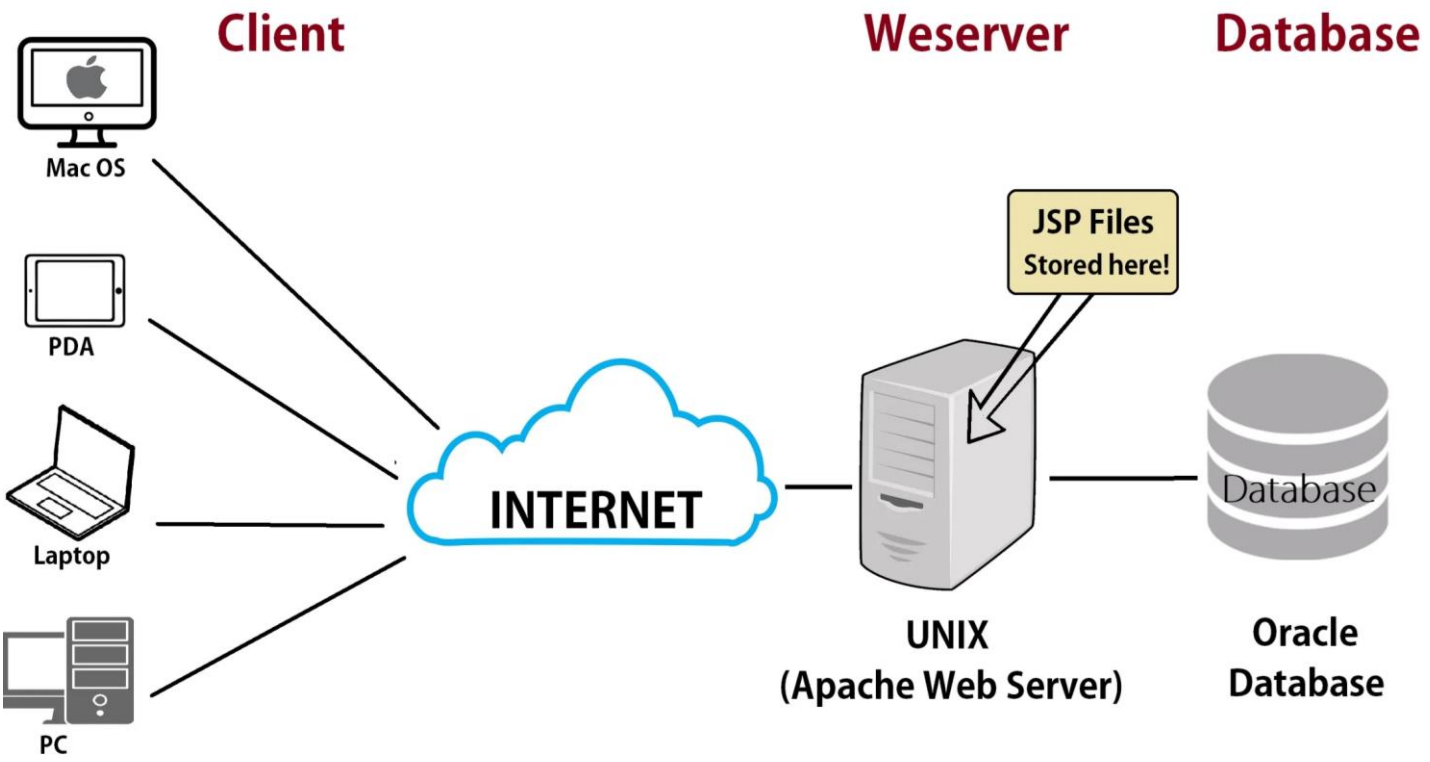
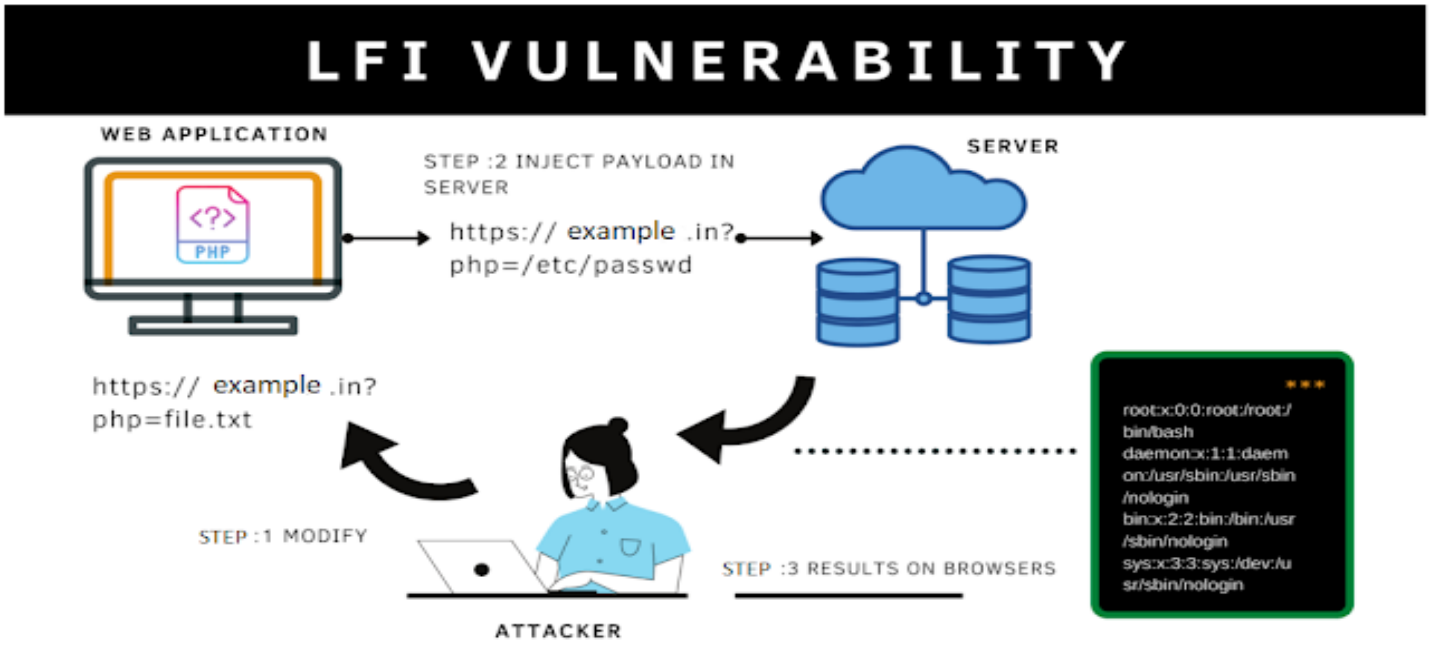




Web Server & LFI

ARENA WEB SECURITY

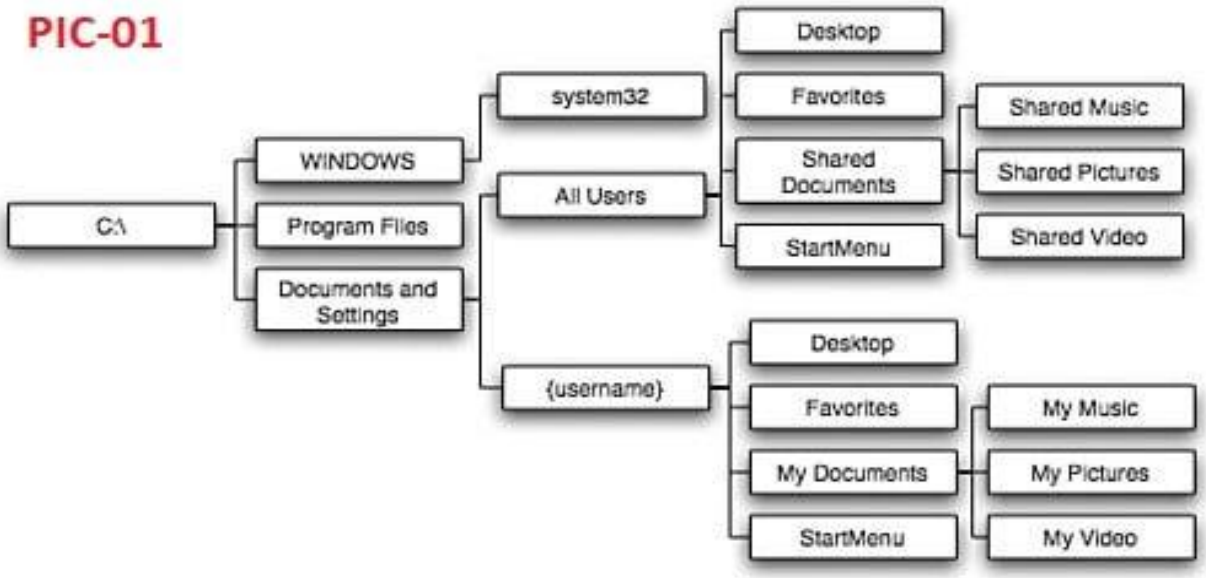
আসুন জেনে নেই

ওয়েভ সার্ভারঃ

ওয়েভ সার্ভার ভালভাবে না জনলেও এতোদিন ওয়েভ সাইট ঘাটতে ঘাটতে ওয়েভ সাইট সম্পর্কে অনেকটা ধারনা অল-রেডি পেয়েছি। ওকে, ওয়েভ সাইট থাকে কোথায়? ওয়েভ সাইট থাকে ওয়েভ সার্ভারে। তো, সেই সার্ভার টি আসলে কি? সেটাও একপ্রকার হাই-ইন্ড কম্পিউটার, গেমিং পিসির মতো এই টাইপ পিসির প্রসেসর (ইন্টেল এর হলো জিয়ন Xeon, আর AMD এর হলো EPYC, তবে সার্ভারে ইন্টেল ই বেশী ব্যবহৃত হয়), মাদারবোর্ড, পাওয়ার সাপ্লাই এমন কি কেসিং ও আলাদা, ও হ্যাঁ- সার্ভারের অপারেটিং সিস্টেম ও কিন্তু আলাদা। সার্ভারের অপারেটিং সিষ্টেম হিসাবে লিনাক্স বা উইন্ডোজ ব্যবরহৃত হলেও লিনাক্সের সিষ্টেমের সিকিউরিটি সিস্টেম অনেক বেশী শক্তিশালী হওয়াতে লিনাক্স সার্ভার ই বেশী্ পাশাপাশি ওয়েভ সার্ভার হিসাবে উইন্ডোজ ব্যবহার করে আই আই এস Internet Information Services (IIS) অন্যদিকে লিনাক্স এ apache server (এ্যপাচি সার্ভার)।

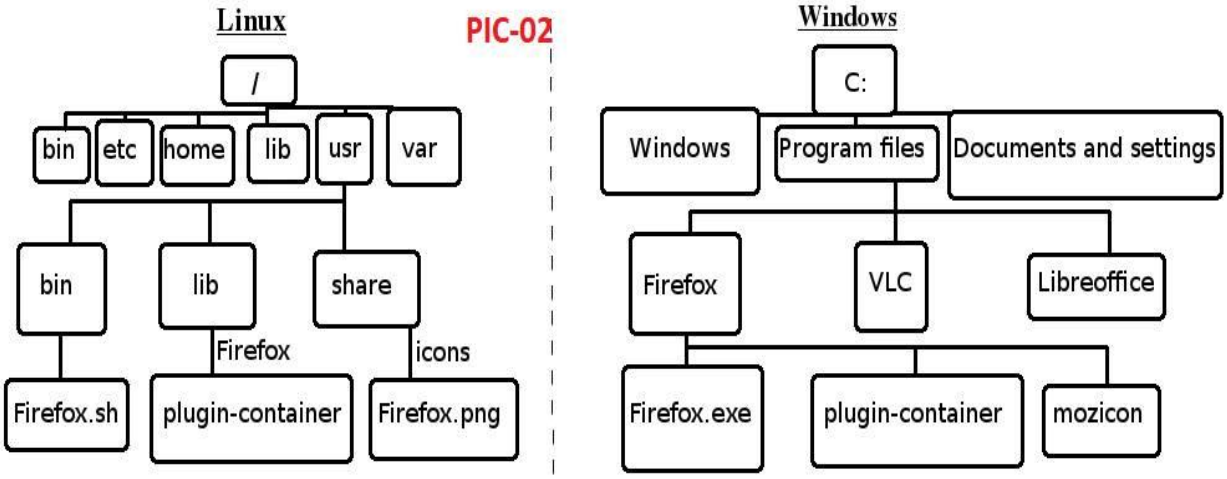
উইন্ডোজ এর ফাইল ষ্ট্রাকচার তো আমরা জানিই, কেননা আমাদের সবচেয়ে বেশী ব্যবহার করা পিসি বা ল্যাপটপটি উইন্ডোজের, এই উইন্ডোজ 7-10-11 এর ইন্টারফেস ও ফোল্ডার এর মতোই সেইম উইন্ডোজ সার্ভার-2016, উইন্ডোজ সার্ভার-2018, উইন্ডোজ সার্ভার-2022 এ।

- ছবি টি দেখে নিন।



লিনাক্স যেহেতু দেখিনি তাহলে লিনাক্সের ডিরেক্টরী(আরে টেনশন নিয়েন না- উইন্ডোজে যিনি ফোল্ডার আর লিনাক্সে এসে উনি হয়েছেন ডিরেক্টরী) , ফাইল ষ্ট্রাকচার টা একটু দেখে নেই।

📷 ছবি টি দেখে নিন।



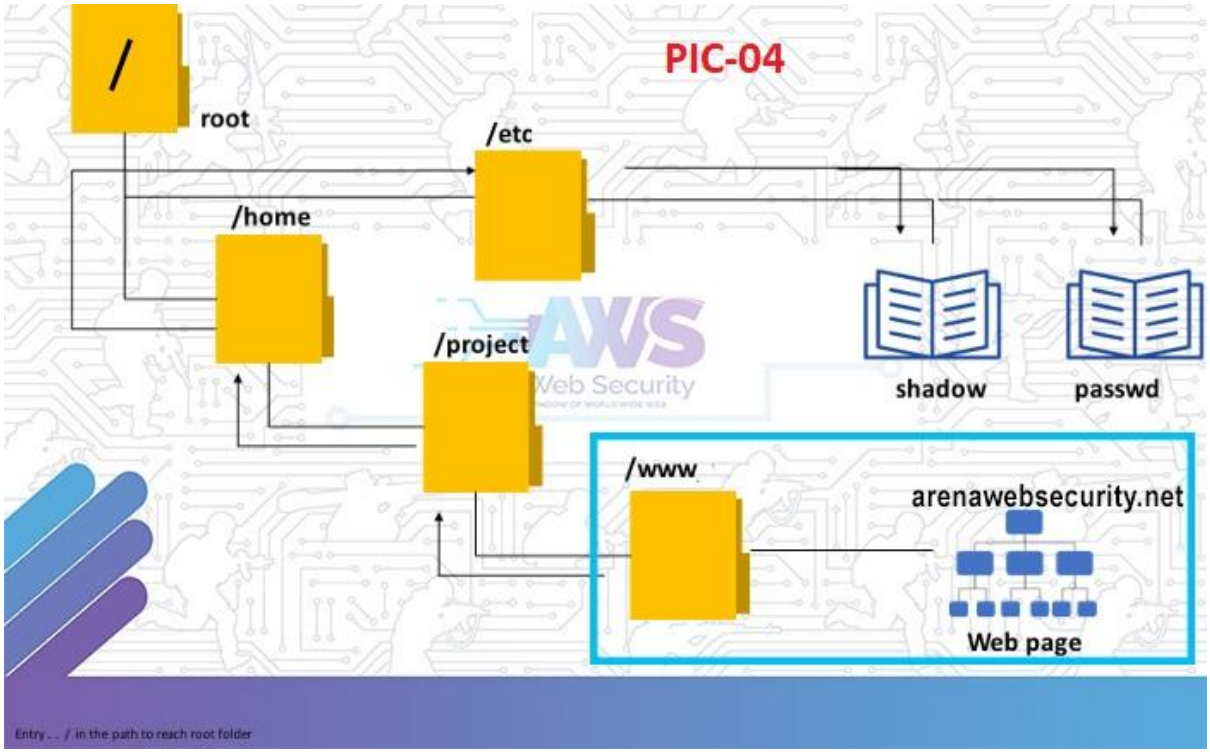
লিনাক্সের রুট ডিরেক্টরী এবং ওয়েভসার্ভারের রুট ডিরেক্টরী কি একই?

না , লিনাক্সের রুট হলো সমস্ত ডিরেক্টরীর মেইন, / চিহ্ন দিয়ে রুট ডিরেক্টরী বোঝানো হয়, তার আন্ডারে অন্যান্ন সব ডিরেক্টরী, ডিরেক্টরীর অধীনে সাব ডিরেক্টরী, ফাইল থাকে। যেমন উইন্ডোজের ক্ষেত্রে যদি সি ড্রাইভ কে রুট ধরি, তাহলে তার আন্ডারে বিভিন্ন ফোল্ডার, ফোল্ডারের অধীনে সাব ফোল্ডার, ফাইল থাকে।

উইন্ডোজে যখন কোন সফ্টওয়্যার ইন্সটল করি তখন বাই ডিফল্ট সেটা C:\Program Files বা C:\Program Files (x86) এ গিয়ে ইন্সটল হয়, তেমনি লিনাক্সের ওয়েভ সাইট হোষ্টিং এর জন্য ডিফল্ট ডিরেক্টরী হলো /var/www/html, যদিও এখন অনেকে সিকিউরিটি পারপাসে কাষ্টম ইন্সটল করে(যেমনঃ /home/ বা /home1/(custom Directory name)/www/ বা /home/(custom Directory name)/domains/ এই টাইপের) আর এটাই হলো সার্ভারের ওয়েভ সাইটের রুট ডিরেক্টরী। এই ডিরেক্টরীর অধীনে admin ডিরেক্টরী থাকে, resourece direrctories(Images, includes, js, css, থাকে, আরো কত কত সাব ডিরেক্টরী, ফাইল থাকে।

যাই হোক, শেল করার পর বা লিনাক্সে গেলে বিষয়টি আরো ক্লিয়ার হয়ে যাবেন।

আপাতত এতটুকু মনে রাখলেই হবে যে একটি ওয়েভ সাইট এর রুট ডিরেক্টরী আর মেইন সার্ভারের রুট ডিরেক্টরী সেইম না।



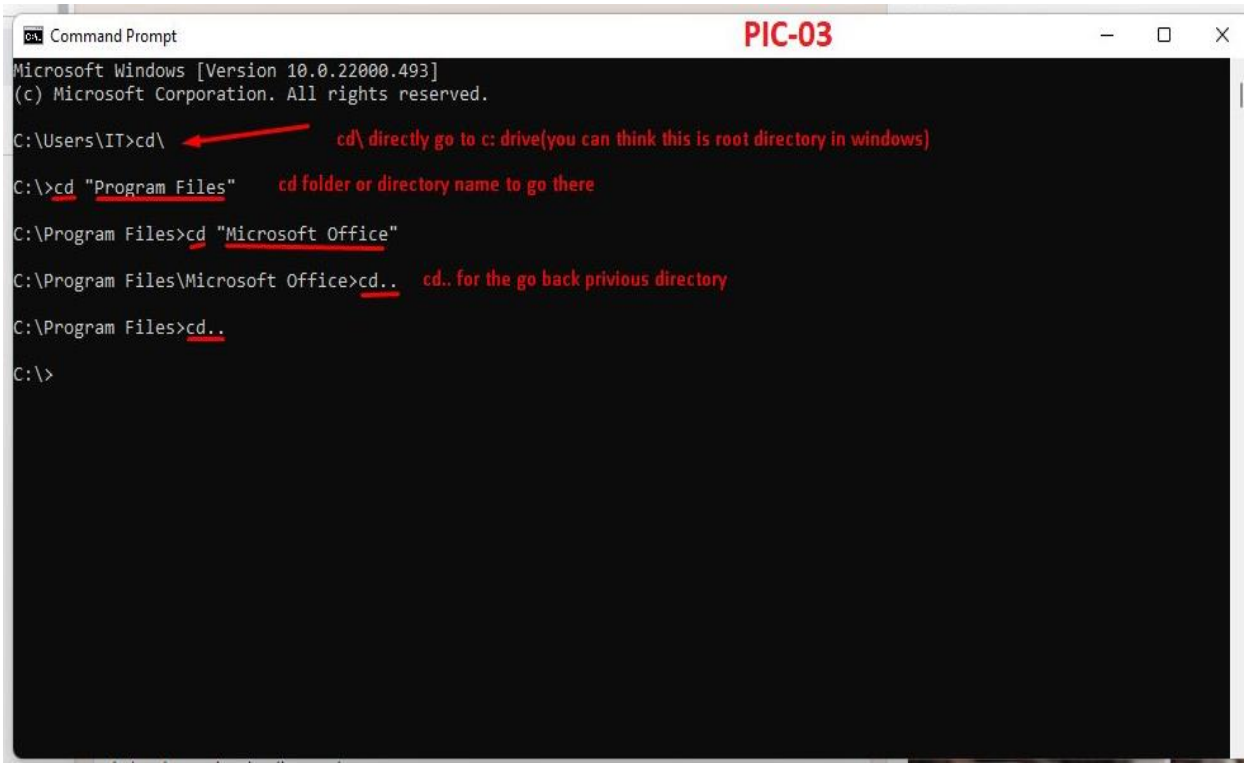
সাথে একটু এডিশন করে দেই- ধরেন আপনি আপনার পিসিতে পোগ্রাম ফাইলস ফোল্ডারে মাইক্রোসফ্ট অফিস ফোল্ডার আছে। যদি সেটা উইন্ডোজ কমান্ড প্রোম্পট থেকে দেখেন তাহলে কেমন দেখাবে?

C:\Program Files\Microsoft Office>, আচ্ছা আপনি ধরেন এই ফোল্ডারে আছেন তাহলে কিভাবে তার আগের ফোণ্ডারে যাবেন?

C:\Program Files\Microsoft Office>cd.. (cd.. কমান্ড দিলেই আগের ফোল্ডারে যেতে পারবেন।) এখন সে দেখাবে C:\Program Files>আবার এখানে cd.. কমান্ড দিলেই আগের ফোল্ডারে মানে সরাসরি সি ড্রাইভে C:\> চলে যেতে পারবেন।

অথবা যদি C:\Program Files\Microsoft Office> এখান থেকে সরাসরি C:\> তে যেতে চান তাহলে cd\ দিয়ে এন্টার করে নিন সরাসরি C:\> তে চলে যাবে। তেমনি লিনাক্সে ডিরেক্টরী পরিবর্তনের জন্য cd.. বা রুট ডিরেক্টরীতে যেতে cd / কমান্ড।

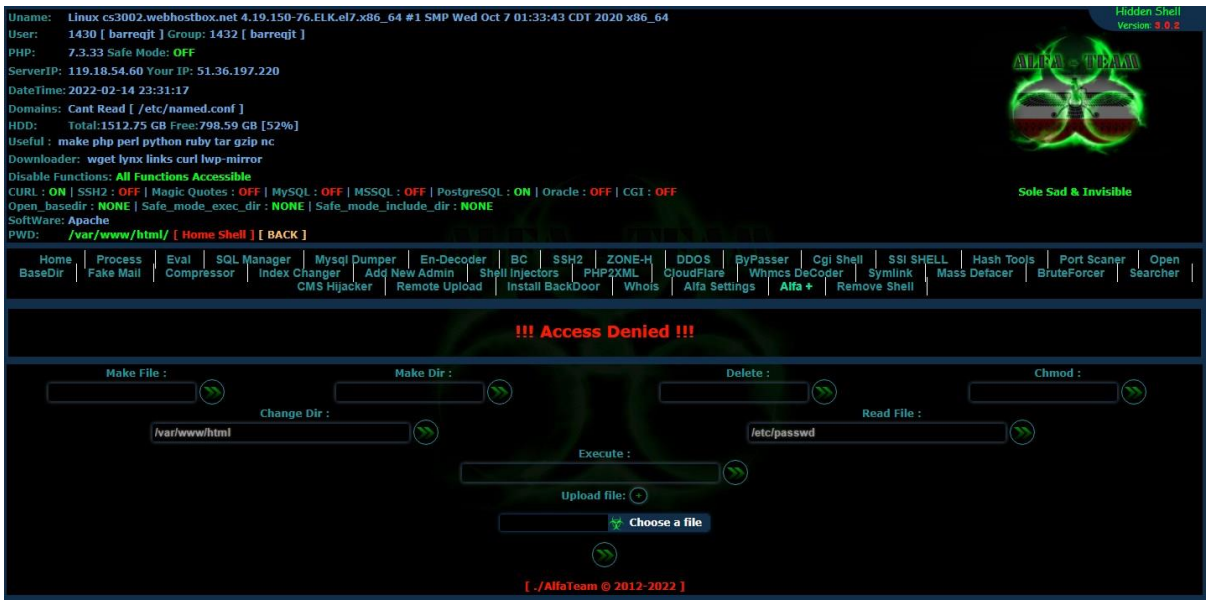
- 📷 ছবি টি দেখে নিন।

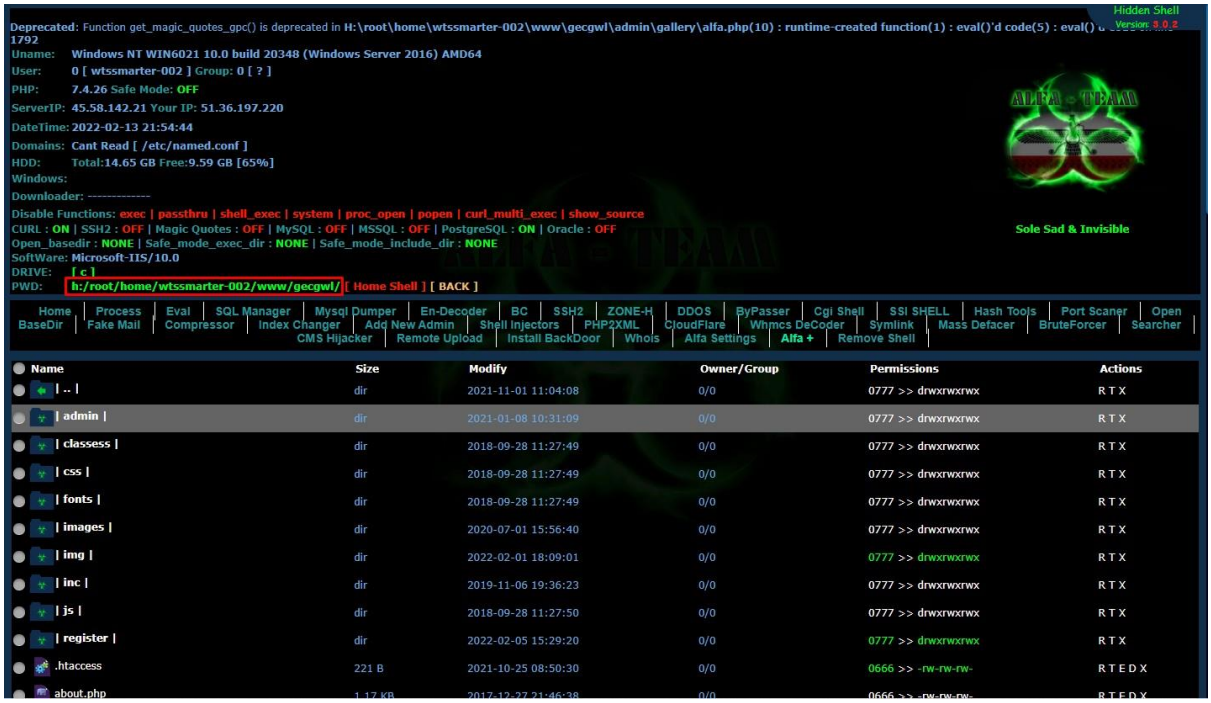


মাথা নষ্ট করার কিছুই নেই, এখন শুধু আইডিয়া টা নেন, এটা লিনাক্সের ক্লাসে বুঝে যাবেন।

(সম্ভব হলে ডস কমান্ড নিয়ে ছোট একটি ভিডিও করে দিবেনে।)

- ছবি টি দেখে নিন।





Local File Inclusion Vulnerability(Lfi):

নিয়ে কিছু বলার আগে ছোট করে বলে দেই- আগে আমরা ওয়েভ সাইটের ভার্নাবেলিটি থেকে ওয়েভ সাইটের তথ্য বরে করেছি বা বা ওয়েভ সাইট এক্সেস বা হ্যাক করেছি। এই পার্টে আমরা দেখবো ওয়েভ সাইটের ভার্নাভেলিটির মাধ্যমে ওয়েভ সার্ভারের গুরুত্ব পূর্ণ তথ্য বের করা। তাতে এমন ও হতে পারে ওয়েব সাইট ও হ্যাক করার পসিবল হতে পারে।

Local File Inclusion Vulnerability(Lfi):

প্রতিটি ওয়েভ সার্ভারে অনেক গুরুত্বপূর্ণ ফাইল থাকে যেমন- সার্ভার কনফিগারেশন ফাইল, ইউজার ফাইল, পাসওয়ার্ড ফাইল ইত্যাদি (যেমনটি থাকতে পারে আপনার পিসিতেও।), এখন যদি ওয়েভ এপ্লিকেশন সার্ভারের সেই লোকাল ফাইলগুলো এনক্লুড করতে পারে এবং সেগুলোর কনটেন্ট দেখা বা পড়া যায় তাহলে বুঝতে হবে সেই ওয়েভ এপ্লিকেশনে লোকাল ফাইল অন্তর্ভুক্তি বা ইনক্লুশন(Lfi) ভারনাবিলিটি রয়েছে।

প্রথমেই মনে রাখতে হবে যে সার্ভারের এই সব ফাইলগুলো অনেক সেনসেটিভ এবং এগুলো ওয়েভ সাইটের মাধ্যমে দেখতে পারার কথা না, এগুলো ওয়েভ ডেভেলাপারদের বাগ। এই বাগটি এতোটাই বড় ধরনের বাগ যে এই বাগের কারনে ওয়েভ সার্ভারটিও হ্যাক হয়ে যেতে পারে।

ইতিপূর্বে ইউ আর এল ও ওয়েভ সাইটের ষ্ট্রাকচার নিয়ে বেশ করেয়কটি পোষ্ট করেছি, ভুলে গেলে আবার পড়ে নিন(গ্রুপেই আছে পোষ্ট গুলো)।

সাপোস কোন একটি ওয়েভ সাইট এর ইউ আর এল বা লিংক টি কেমন হয়?

www.test.com/index.php বা www.test.com/home.php বা www.test.com/cat_id.php?cat=12

আচ্ছা সার্ভারে কোথায় কিভাবে ফাইল-ফোল্ডার(ডিরেক্টরী) থাকে একটু আগেই বলেছি, সেটা বুঝেছেন তো?

যদি বুঝে থাকেন তাহলে বলি- কোন ওয়েভ সাইটের লিংক থেকে যদি ঐ সার্ভারের বা মূল সার্ভারের রুট বা অন্যান্ন ডিরেক্টরীর কোন ফাইল বা তথ্য বের করা যায় তাহলেই সেটা এল এফ আই।। এস কিউ এল ইরর বা নো-রিডাইরেক্ট যেমন ওয়েভ সাইটের বাগ তেমনি এল এফ আই ও হলো ওয়েভ সাইটের বাগ।

বুঝতেই পারছেন- এস কিউ এল, নো-রিডাইরেক্ট যাই বলি না কেন সেসব বাগ দিয়ে বড় জোড় ঐ ওয়েভ সাইট এক্সেস নেয়া যেতে পারে। কিন্তু এল এফ আই বাগ এর কারনে মূল সার্ভারের গোপনীয় তথ্য বের করা যেতে পারে।

কি ভাবে এই ধরনের বাগযুক্ত সাইটকে এক্সপ্লুয়েট করা যায়?

প্রথমে আমাদের এইরকম বাগ থাকতে পারে সেরকম সাইট খুঁজে বের করতে হবে।

তারপর চেষ্টা করতে হবে ওয়েভ সার্ভারের রুট বা অন্যান্ন ডিরেক্টরীর কোন ডাটা পাওয়া যায় কিনা?

মনে আছে ইনফরমেশানল পোষ্ট-৫ এ ডর্কের আগে ইউ আর এল বুঝাতে গিয়ে কি বলেছিলাম? বলেছিলাম প্যারামিটারে একাধিক কুয়েরী থাকতে পারে। আবার আসুন জেনে নেই-৪ এ গেট মেথডে বলেছিলাম- উই আর এল এ পুরো কুয়েরী বা ইনফরমেশনগুলো শো করবে।

তার মানে হলো- এমন অনেক ওয়েভ সাইট পেতে পারি যেখানে এমন কুয়েরী পসিবল-

www.example.com/index.php?file=test.php

এখানে www.example.com/index.php এর কনটেন্ট এক ধরনের কিন্তু test.php এর কনটেন্ট আরেক রকমের, কিন্তু সে test.php এর কনটেন্ট কে কোথা থেকে রিকোয়েষ্ট করছে? করছে ওয়েভ সাইটের ইনডেক্স ফাইল থেকে। এটা কি শুধু index.php থেকেই হাতো? না, ঐ ওয়েভ সাইটের অন্যান্ন পার্ট যেমন www.example.com/home.php?something=something.phpহতে পারে, www.example.com/news.php?something=something.phpও হতে পারে। something মানে কি সেটাও বলা লাগবে? যা কিছুই হতে পরে তবে ওয়েভ কনটেন্ট রিলেটেড লাইক- page, redirect, inc, include, main, pg, cat, content ……..

আচ্ছা আসিফ ভাই তো ডর্ক গ্রুপে দিয়েই দিয়েছে, তাহলে ডর্ক নিয়ে তো প্যারা নেই।।

এক্সপ্লুয়েট কি ভাবে করবো?

ক্লাস ভিডিওটা দেখেন, আগে না বুঝলেও এখন বুঝে যাবেন।