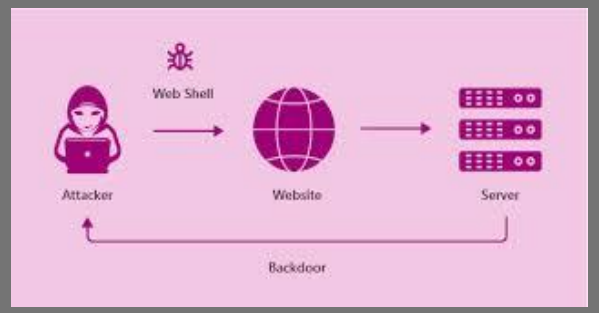
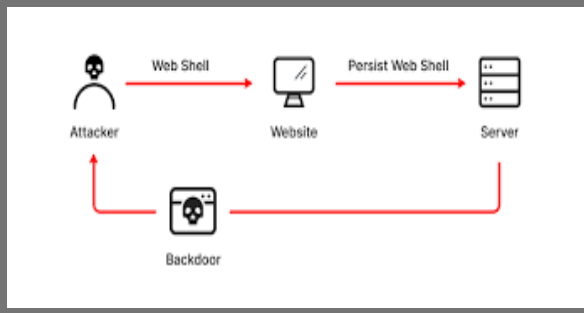
What if a hacker controlled your server…
through a browser?






# Web Shell

## A Hidden Cyber Threat

Seminar-10

# Disclaimer..!

This presentation is intended for **educational** and **ethical purposes only.**

The demonstration of a web shell and associated commands is to raise awareness about server vulnerabilities and teach prevention techniques.

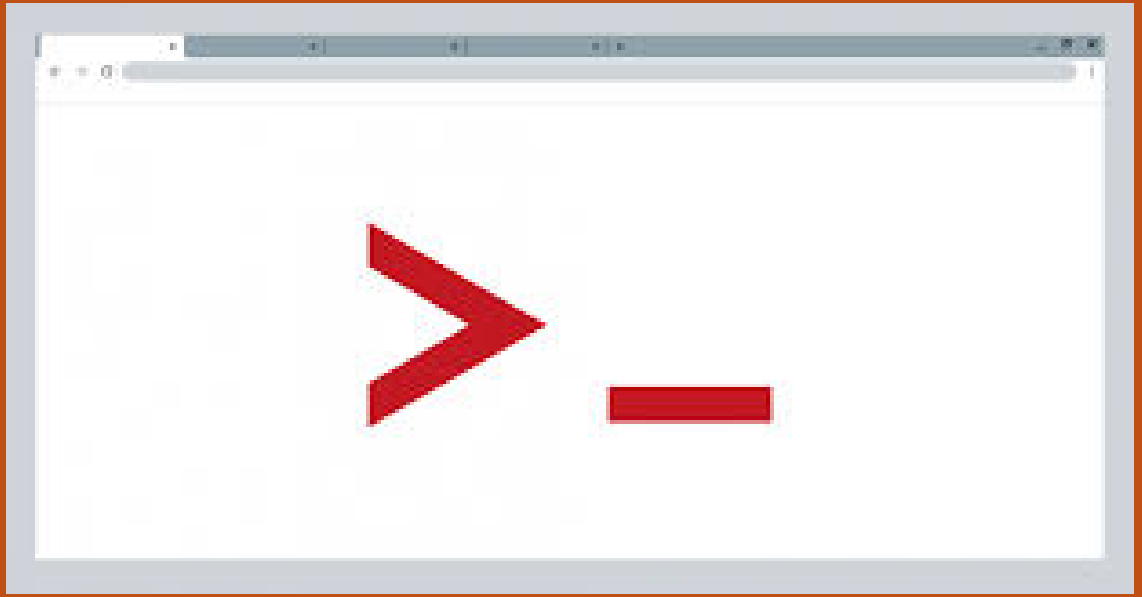
**Do not attempt to use these techniques on any system without proper authorization.**

**Unauthorized access or exploitation of systems is illegal and unethical.**

The presenter and organizers do not condone or take responsibility for misuse of this information.

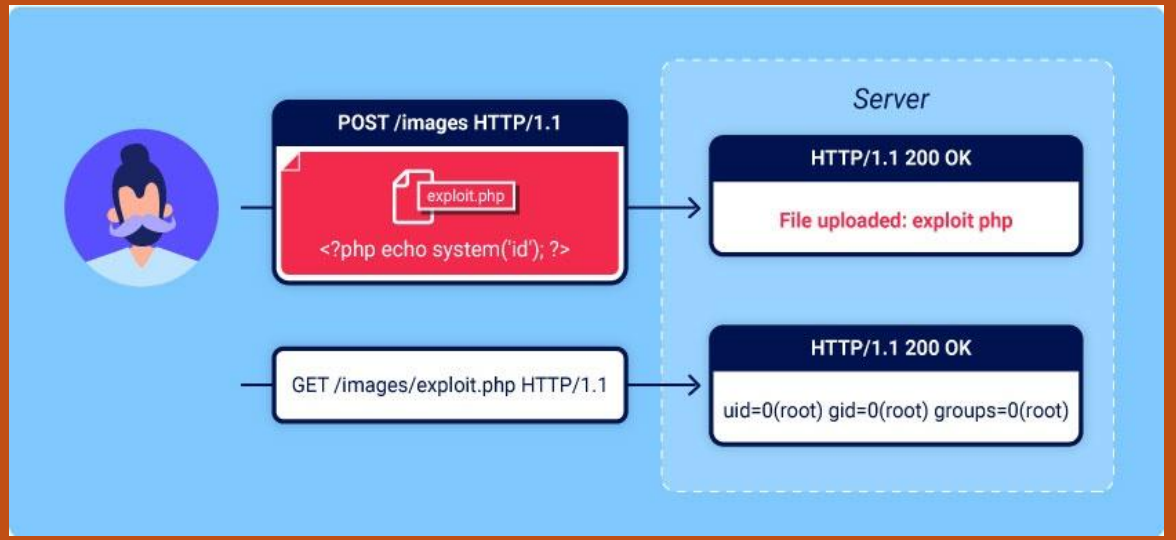
# What is Web shell?

**A web shell is a malicious script that provides remote access to a compromised server via a web interface.**



# Step 1: Attacker finds vulnerability


**Browser Plugin**




**Unprotected file Upload**

# Step 2:Server then process the file

# Step 3: Accesses the Web Shell via Browser

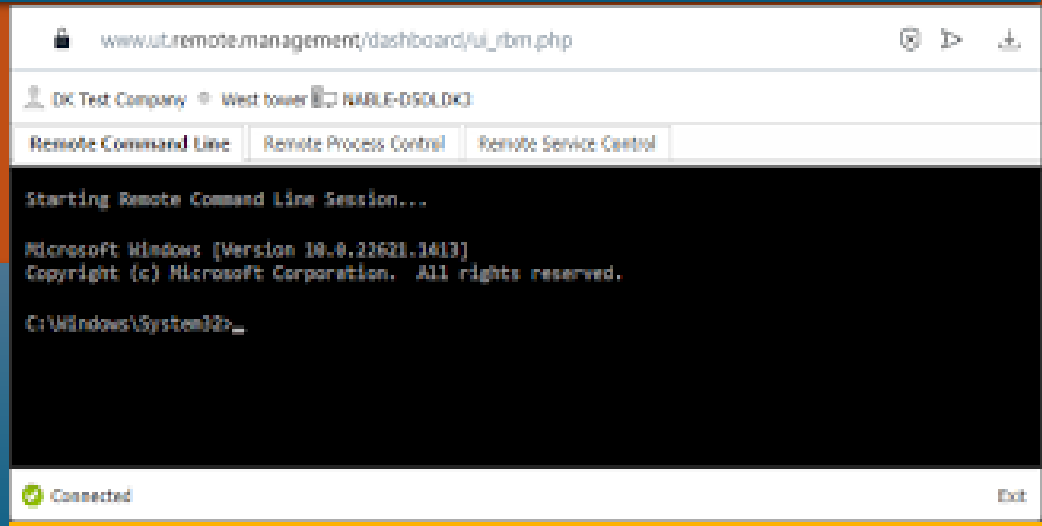

**Attacker opens uploaded file in browser**

**http://victimsite.com/uploads/shell.php?cmd=whoami**

# Step 4: Executes System Commands

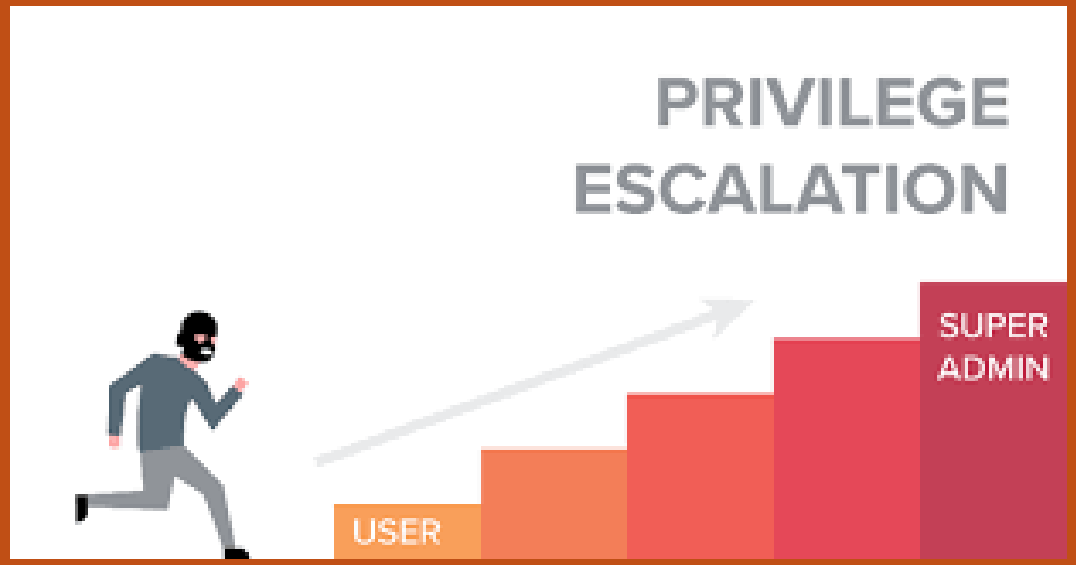
Once the access is gained, attacker can:

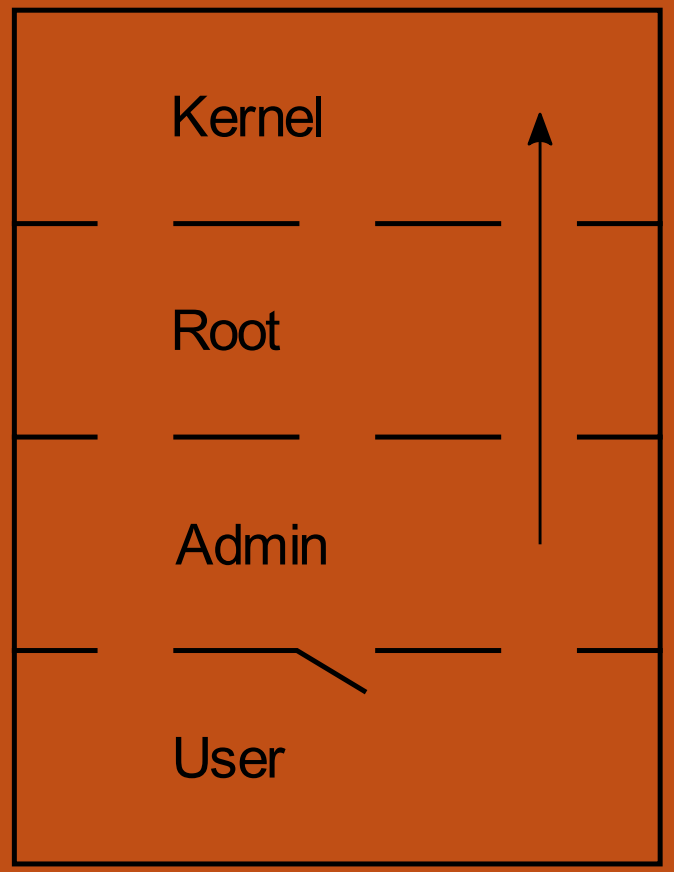
- Run commands (ls, cat, pwd)
- Browse files
- Add new users
- Modify or delete data
- Even install malware or ransomware




# Step 5: Stays Hidden or Escalates

- Web shells can be renamed to innocent-looking files (`image.php`, `update.php`)
- Used to maintain **persistence** or create a **reverse shell** for deeper access.




**Source:** Wikipedia

# Practical session

**Tools/languages used:**

- Xampp/lamp
- Php
- Web browser

# Real world impacts & detection

Some of the real world impacts include **data exfiltration, lateral movements in network, long term persistence** etc.

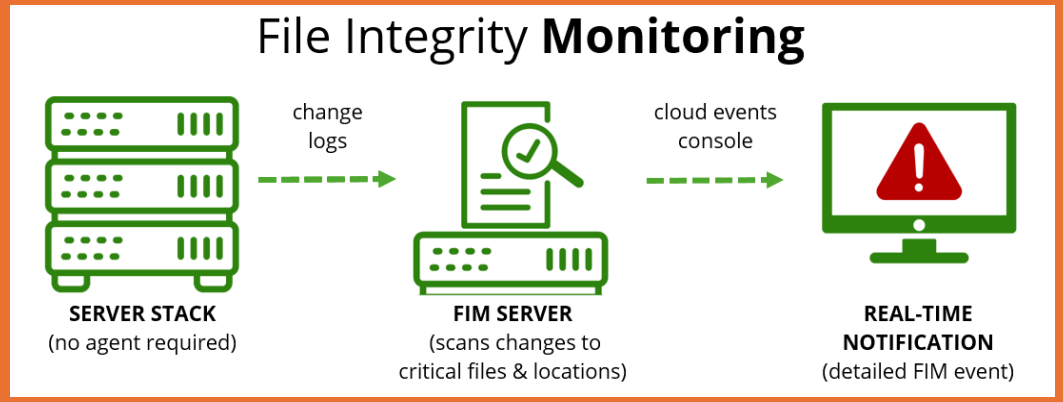
**Detection can be done by:**

## 1) Unusual HTTP Requests

http://nxixipcfj/image.php

http://jgdgrlnncg/

http://uxucserkokwfr/


## 2) File Integrity Monitoring (FIM)

**`/var/www/html/` (for web servers like Apache)**

**Configuration files (e.g., `/etc/`)**

**System binaries (e.g., `/bin/`, `/usr/bin/`)**

# Thank you


Security warning
INSIDE JOBS
59%
of employees steal proprietary corporate data when they
quit or are fired