1. Tes
2. Tes
3. Code Based Questions:
4. <?php

$string = "Hello, World!";

$jumlahKarakter = strlen($string);

echo "Jumlah karakter dalam string: " . $jumlahKarakter;

?>

1. Pertama, buka file application/config/database.php dan sesuaikan pengaturan database seperti di bawah ini:

$db['default'] = array(

'dsn' => '',

'hostname' => 'localhost', // ganti dengan host MySQL Anda

'username' => 'username', // ganti dengan username MySQL Anda

'password' => 'password', // ganti dengan password MySQL Anda

'database' => 'database\_name', // ganti dengan nama database Anda

'dbdriver' => 'mysqli',

'dbprefix' => '',

'pconnect' => FALSE,

'db\_debug' => (ENVIRONMENT !== 'production'),

'cache\_on' => FALSE,

'cachedir' => '',

'char\_set' => 'utf8',

'dbcollat' => 'utf8\_general\_ci',

'swap\_pre' => '',

'encrypt' => FALSE,

'compress' => FALSE,

'stricton' => FALSE,

'failover' => array(),

'save\_queries' => TRUE

);

1. function calculateTotalPrice(array $items, float $taxRate, float $discount): float {

$subtotal = 0;

foreach ($items as $item) {

$price = $item['price'];

$quantity = $item['quantity'];

$subtotal += ($price \* $quantity);

}

$totalWithTax = $subtotal + ($subtotal \* $taxRate);

$totalWithDiscount = $totalWithTax - ($totalWithTax \* $discount);

return round($totalWithDiscount, 2);

}

1. Pertanyaan Keamanan
2. Apa itu serangan CSRF (Cross-Site Request Forgery) dan bagaimana caranya

melindungi aplikasi PHP dari serangan ini?

Serangan yang memanfaatkan bahwa web tidak adanya verifikasi/authentikasi permintaan yang dikirim dari sumber yang sah

salaah satu cara melindungi aplikasi php dengan cara membuat token csrf pada setiap form yang ada.

1. Menjelaskan konsep hashing dan enkripsi dalam konteks password

penyimpanan dan berikan contoh penerapan kode validasi

1. Jelaskan serangan injeksi SQL dan cara mencegahnya dalam kode PHP

Serangan yang penyerang untuk memasuk kode sql berbahaya ke input yang tidak ada verifikasi/ tidak ada validasi untuk menyaring inputan user dengan benar, dan memanipulasi query yang di ekse oleh server database

Untuk mencegahnya dengan cara :

* Tidak memberikan atau membatasi informasi kepada user
* Mengupdate frame atau library yang dipakai
* Gunakan pengaman di databse dengan memakai konfigurasi pengaturan yang keamanan
* Gunakan parameter binding contoh

$stmt->bindParam(':username', $username);

$stmt->bindParam(':password', $password);

* Validasi user dengan membersihkan input yang sudah terkirim

$username = mysqli\_real\_escape\_string($conn, $\_POST['username']);

$password = mysqli\_real\_escape\_string($conn, $\_POST['password']);