

Week 7 - Praktikum Pemrograman Lanjut A

NAMA : Patra Ananda  
NIM : 10241061

SOAL :

1. Builder Pattern - Validator Class

- Extend Validator.php dengan 6 validation rules baru:
  - numeric() - Validasi angka (int/float)
  - between(\$min, \$max) - Nilai antara min-max
  - in(\$array) - Nilai dalam whitelist array
  - unique(\$table, \$column, \$exceptId) - Unique check di database
  - confirmed(\$field) - Field sama dengan {field}\_confirmation
  - dateFormat(\$format) - Validasi format tanggal

Deliverable: Validator digunakan minimal di 2 controller (Patients & Appointments)

2. Factory Pattern - Multi-Entity

A. AppointmentFactory - Buat class dengan 5 methods:

- create(), createMany(), createForPatient(), createForDoctor(), createInRange()

Data realitis: schedule weekday 08:00-17:00, duration 30-60 menit, valid patient/doctor IDs

B. DoctorFactory - Buat class dengan 4 methods:

- create(), createMany(), createBySpecialization(), createWithSchedule()

Nama: "Dr. Ahmad, Sp.PD", Email: dr.firstname@hospital.com, Phone Indonesia

:Update seed.php untuk seed 50 patients + 20 doctors + 100 appointments

3. Week 6 Enhancement - Recycle Bin

A. Auto-Delete - Tambahkan method autoDeleteOld(\$days = 30) di Repository:

- Hard delete records yang deleted\_at > 30 hari lalu
- Controller action + flash message berapa record terhapus

B. Bulk Restore - Implementasi bulk action:

- View: checkbox per row + "Select All" + button "Restore/Delete Selected"
- Repository: method restoreBulk(\$ids) dan forceDeleteBulk(\$ids)
- Controller: action dengan validasi array IDs

4. Helper Classes (10%)

A. Sanitizer Enhancement (6%) - Tambahkan 3 methods:

- phone(\$value) - Format +62-XXX-XXXX-XXXX
- name(\$value) - Capitalize, hapus angka/special chars
- alphanumeric(\$value) - Only letters & numbers

B. DateHelper (4%) - Buat class baru dengan 5 methods:

- format(\$date, \$format), age(\$birthdate), diffHuman(\$date), toMysql(\$date), isWeekend(\$date)

CSRF Protection

- Implementasi Csrf.php di minimal 3 form (create/edit patients, create appointments)
- Verifikasi token di controller:  
Csrf::verifyOrFail(\$\_POST['csrf\_token'])
- Test attack: buat csrf-test.html external form tanpa token (harus ditolak 403)
- Screenshot token di inspect element + hasil test

JAWAB :

1. Harus menggunakan Kata kata untuk nama supplier, tidak boleh menggunakan simbol

Tambah Supplier Baru

[Dashboard](#) / [Supplier](#) / Tambah

Nama Supplier \*

PT. Supplier Motor

Nama supplier harus diisi

Telepon \*

+62-813-5131-954

Kota

Bandung

Alamat

Alamat lengkap supplier...

← Kembali

Simpan Supplier

Contact Person

Nama kontak

Email

email@supplier.com

2. Helper Classes phone(\$Value) Format +62 XXX XXX XXX





Data Pelanggan

+ Tambah Pelanggan

Cari berdasarkan nama, telepon, atau email...

Cari

Total: 44 pelanggan

No	Nama	Telepon	Email	Alamat	Kota	Aksi
41	Kasus	+62-812-3342-23	palasa@gmail.com	Jl. Soekarno Hatta No.KM 15, Karang Joang, Kec. Balikpapan Utara, Kota Balikpapan, Kalimantan Timur 76127	Kota Balikpapan	 
42	Kusikam	+62-813-5423-6785	KUSIK@gmail.com	jl 12	Bandung	 

3. Auto-Delete dan Bulk Restore

Recycle Bin - Produk Terhapus

Kembali ke Produk

Kembalikan Semua







Auto-Delete (> 30 hari)

Kosongkan Recycle Bin

Select All (0 selected)


Restore SelectedDelete Selected

Total: 3 produk di Recycle Bin

No	Kode	Nama Produk	Kategori	Dihapus Pada	Aksi
1	SPR0005	Spion Lipat 5	Velg Racing	02/11/2025 01:58 (-1 hari yang lalu)	 
2	SPR0004	Cover Body 4	Knalpot	02/11/2025 01:58 (-1 hari yang lalu)	 
3	AS22	Velg Racing222	Ban	02/11/2025 01:58 (-1 hari yang lalu)	 

4. Hard delete > 30 hari

Informasi: Auto-delete akan menghapus produk yang sudah lebih dari 30 hari di Recycle Bin.



Tidak ada produk yang perlu dihapus otomatis  
Semua produk di Recycle Bin masih kurang dari 30 hari

Kembali ke Recycle Bin

Ke Dashboard

5. Csrf-test.php

**⚠ WARNING: Malicious Form Detected!**

Form ini mencoba mengirim data ke server **TANPA CSRF TOKEN**. Jika server tidak dilindungi, data akan masuk ke database!

**🔒 Malicious Form (No CSRF Protection)****🚀 Inject Fake Product**

Category ID:

Supplier ID:

Product Code:

Product Name:

Price (Rp):

Stock:

❌ **MISSING:** `<input type="hidden" name="csrf_token" value="176aabef0d1444148b7b6f157992507ef84c4d9e148a101e9389b3f44824d919">`

**🚀 LAUNCH CSRF ATTACK (Should FAIL with 403)**

6. Isi data tanpa Token akan ditolak diluar website Csrftest.php



## 7. Isi data dengan menggunakan Token

### 1 CSRF Token di Session

🔍 **Untuk Screenshot:** Buka Developer Tools (F12) → Application → Session Storage → localhost

Token: 176aabef0d1444148b7b6f157992507ef84c4d9e148a101e9389b3f44824d919

### 2 Form dengan CSRF Token (VALID)

✅ **Expected Result:** Submit berhasil, data tersimpan

Nama Kategori:

PAKAI TOKEN

Deskripsi:

Kategori ini dibuat dengan CSRF token yang valid

🔑 **CSRF Token (Hidden Input):**

```
<input type="hidden" name="csrf_token" value="176aabef0d1444148b7b6f157992507ef84c4d9e148a101e9389b3f44824d919">
```

✓ Submit dengan Token (HARUS BERHASIL)

8. Dan hasilnya bisa dimasukan karena dapat token dari dalam website

























Data Kategori

+ Tambah Kategori

Cari berdasarkan nama kategori atau deskripsi...

Cari

Total: 12 kategori

No	Nama Kategori	Deskripsi	Tanggal Dibuat	Aksi
1	Ban	Ban motor berbagai merk	07/10/2025	 
2	Body Motor	biar cakep dibawahnya	07/10/2025	 
3	Knalpot	Knalpot racing dan standar	07/10/2025	 
4	Knalpot sajaro		02/11/2025	 
5	Lampu Biled	kasih terang motor mu itu	07/10/2025	 
6	Mesin Motor	Mesin Motor Racing	07/10/2025	 
7	PAKAI TOKEN	Kategori ini dibuat dengan CSRF token yang valid	02/11/2025	 
8	Pengereman	buat motor mu aman	07/10/2025	 
9	Spion	Spion motor berbagai model	07/10/2025	 
10	Suspensi Shock	biar empuk itu motor mu ces	07/10/2025	 
11	Velg BSD		02/11/2025	 
12	Velg Racing	Biar ganteng dibawah	07/10/2025	 

12

Implementasi Pada Project Motor Variasi

1. Builder Pattern – Validator Class

Tujuan di Website

Membuat sistem validasi form yang bisa disusun secara berantai (chainable), supaya mudah dibaca dan bisa digunakan di banyak form (produk, pelanggan, supplier, dll).

Sebelum Builder Pattern

```
if (empty($_POST['price'])) {
    $errors[] = 'Harga wajib diisi';
}
if (!is_numeric($_POST['price'])) {
    $errors[] = 'Harga harus berupa angka';
}
if ($_POST['price'] < 1000 || $_POST['price'] > 10000000) {
    $errors[] = 'Harga di luar batas yang diperbolehkan';
}
```

Sesudah Builder Pattern

```
$validator->field('price')
    ->required()
    ->numeric()
    ->between(1000, 10000000);
```

### Efek di Website

- Form validasi di semua halaman jadi seragam.
- Developer tinggal “membangun” aturan seperti berbicara.
- Gampang tambah aturan baru (misalnya `unique()` atau `confirmed()`).

---

## 2. Factory Pattern – ProductFactory & CustomerFactory

### Tujuan di Website

Menyederhanakan proses insert data produk dan pelanggan tanpa menulis ulang SQL di setiap controller.

### Sebelum Pakai Factory

```
$sql = "INSERT INTO products (name, price) VALUES (?, ?)";
$stmt = $db->prepare($sql);
$stmt->bind_param("si", $data['name'], $data['price']);
$stmt->execute();
```

### Setelah Pakai Factory

```
$productFactory = new ProductFactory($db);
$productFactory->create([
    'name' => 'Vario 150 Spare Part',
    'price' => 250000,
    'supplier_id' => 3
]);
```

### Efek di Website

- Tambah produk baru cukup satu baris kode.
- Bisa generate data dummy untuk testing.
- Semua logika insert tersentralisasi, jadi lebih aman dan efisien.

---

## 3. Recycle Bin – Auto Delete dan Bulk Restore

### Tujuan di Website

Fitur Recycle Bin seperti “tempat sampah” di admin panel. Saat produk dihapus, data tidak langsung hilang, tapi diberi timestamp `deleted_at`.

### Auto Delete (>30 Hari)

```
$products = $db->query("
    SELECT * FROM products
    WHERE deleted_at < DATE_SUB(NOW(), INTERVAL 30 DAY)
");
foreach ($products as $p) {
    if (!hasTransaction($p['id'])) {
        unlink("uploads/{$p['image']}");
        $db->query("DELETE FROM products WHERE id = {$p['id']}");
    }
}
```

### Bulk Restore

#### Frontend (JavaScript):

```
let selected = [];
function toggleSelect(id) {
    if (selected.includes(id)) selected = selected.filter(x => x !== id);
    else selected.push(id);
}
```

#### Backend (PHP):

```
$ids = array_map('intval', json_decode($_POST['ids']));
$sql = "UPDATE products SET deleted_at = NULL WHERE id IN (" . implode(',', $ids)
. ")";
$db->query($sql);
```

### Efek di Website

- Admin bisa pilih banyak data sekaligus dan klik “Restore”.
- UI terasa modern (ada “Select All”, jumlah terpilih, dll).
- Menggunakan transaksi untuk keamanan data.

## 4. Helper Classes

### A. Sanitizer

```
class Sanitizer {
    public static function phone($value) {
        $value = preg_replace('/[^0-9]/', '', $value);
        return '+62-' . substr($value, 1, 3) . '-' . substr($value, 4);
    }
    public static function name($value) {
        return ucwords(preg_replace('/[^a-zA-Z\s]/', '', $value));
    }
    public static function alphanumeric($value) {
        return preg_replace('/[^a-zA-Z0-9]/', '', $value);
    }
}
```

## B. DateHelper

```
DateHelper::diffHuman('2024-10-15'); // Output: "18 hari yang lalu"
DateHelper::isWeekend('2024-11-02'); // Output: true
DateHelper::format('2024-11-02', 'd/m/Y'); // Output: "02/11/2024"
```

---

## 5. CSRF Protection

### Tujuan di Website

Untuk mencegah Cross-Site Request Forgery (form palsu dari luar situs).

#### HTML View:

```
<form method="POST" action="save.php">
    <?= csrf::field() ?>
    <input type="text" name="name">
    <button type="submit">Simpan</button>
</form>
```

#### Controller:

```
public function store() {
    csrf::verifyOrFail($_POST['csrf_token'] ?? '');
}
```

### Efek di Website

- Hanya form asli dari situs yang bisa dikirim.
- Form palsu dari situs luar ditolak (403 Forbidden).



- Semua form admin jadi lebih aman.

---

## Kesimpulan

Fitur	Dampak di Website
Builder Pattern	Validasi form jadi rapi dan reusable
Factory Pattern	Insert data lebih mudah & aman
Recycle Bin	Data bisa dipulihkan, tidak langsung hilang
Helper Classes	Input & tanggal lebih bersih dan otomatis
CSRF Protection	Form 100% aman dari serangan eksternal

---

semua pattern ini membuat website lebih cepat dikembangkan, aman, dan mudah di-maintain.