INFORME DE VULNERABILIDAD: INYECCIÓN SQL EN DVWA

---

1. **Introducción**
Este informe detalla la vulnerabilidad de **SQL Injection** detectada en la plataforma **Damn Vulnerable Web Application (DVWA)**. Se describen los hallazgos, el impacto, las técnicas utilizadas para la explotación y las recomendaciones para mitigar este tipo de ataques.

---

2. **Descripción de la Vulnerabilidad**
La inyección SQL es una vulnerabilidad que permite a un atacante manipular consultas SQL ejecutadas por una aplicación web. En DVWA, el módulo de **SQL Injection** permite la ejecución de consultas maliciosas debido a la falta de validación y sanitización de entradas.

Evidencia:
- Se ingresó el siguiente payload en el campo de "User ID":
  ```sql
  ' OR '1'='1
  ```
- La aplicación devolvió todos los registros de la base de datos, incluyendo:
  - ID: admin, Nombre: admin
  - ID: Gordon, Nombre: Brown
  - ID: Hack, Nombre: Me
  - ID: Pablo, Nombre: Picasso
  - ID: Bob, Nombre: Smith

---

3. **Impacto de la Vulnerabilidad**
Esta vulnerabilidad puede tener graves consecuencias, incluyendo:

- **Exposición de datos sensibles:** Un atacante puede obtener información confidencial almacenada en la base de datos.
- **Manipulación de datos:** Posibilidad de modificar, eliminar o insertar datos maliciosos.
- **Escalada de privilegios:** En algunos casos, un atacante puede obtener acceso administrativo al sistema.
- **Compromiso del servidor:** Si la inyección permite la ejecución de comandos del sistema, puede llevar a la toma de control total del servidor.

---

4. **Métodos de Explotación**
Los siguientes métodos pueden ser utilizados para explotar la vulnerabilidad:

a) **Obtención de todos los usuarios**
```sql
```

```
' OR '1'='1
```

b) **Bypass de autenticación**
```sql
' OR '1'='1' --
```

c) **Enumeración de columnas**
```sql
' UNION SELECT null, table_name FROM information_schema.tables --
```

d) **Obtención de credenciales**
```sql
' UNION SELECT username, password FROM users --
```

---

5. **Recomendaciones y Soluciones**
Para mitigar esta vulnerabilidad, se recomienda:

Validación y sanitización de entradas**
- Utilizar funciones como `htmlspecialchars()` y `mysqli_real_escape_string()`.

Principio de menor privilegio**
- Limitar los permisos del usuario de base de datos para evitar ejecución de comandos peligrosos.

Implementación de un WAF (Web Application Firewall)**
- Herramientas como ModSecurity pueden detectar y bloquear intentos de inyección SQL.

Comandos utilizados en la respectiva auditoria.
Se realizará un listado de cada uno de los comandos utilizados en la presente auditoria a fin de que se transparente aun mas el trabajo realizado y evidencia cada uno de los pasos a seguir.
- nmap- sV (detección de servicios de puertos)
- nmap -p 1-200 IP (escaneo por rangos de puertos)
- nmap -sn IP -oN escaneo_hosts.txt (Descubrimiento de host (Ping Sweep))
- nmap -sS -sU -p- -T4 -oN escaneo_tcp_udp.txt 192.168.1.1 (Escaneo de Puertos TCP

6. **Conclusión**
La vulnerabilidad de inyección SQL en **DVWA** demuestra cómo una aplicación web insegura puede exponer información crítica. Implementando las medidas de seguridad recomendadas, es posible mitigar este riesgo y proteger la base de datos de ataques malintencionados.

Estado de la vulnerabilidad: [ ] No mitigada [X] Mitigada

Fecha del informe: [14/02/2025] Hora[20:22]
Autor: [Borja Gómez Sanz]