Informe de vulnerabilidad mediante Inyección de SQL

El siguiente reporte identifica una vulnerabilidad mediante una inyección SQL en la Damn Vulnerable Web Application (DVWA). La prueba se realizó en un entorno controlado.

Descripción del incidente

Durante la prueba de seguridad en DVWA, se descubrió una vulnerabilidad en la sección “inyección de SQL”. Esta permite al atacante engañar a la base de datos para que valide una condición como verdadera

Método utilizado

Se utilizó la siguiente inyección SQL en el campo de “User ID” para demostrar la vulnerabilidad:

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

Esta inyección de código maliciosa lo que intenta es que la condición siempre sea verdadera al escribir ‘1’=’1’. Generando así que la base de datos diga “la condición se cumple” y entregando al atacante los datos que estaba buscando.

Impacto del incidente

Explotando esta vulnerabilidad el atacante es capaz de:

- Acceder a los datos que se encuentran en la base de datos.
- Destrucción o alteración de datos.

Recomendaciones

1) Implementación de la validación de entradas o whitelist. Limitando la cantidad de caracteres y rechazando cualquier entrada que tenga símbolos sospechosos como -- , ; , o UNION. especificando el tipo de dato, si se espera un ID, asegurarnos de recibir un integer.
2) Aplicar el principio de menor privilegio, evitamos que usuarios tengan acceso a permisos como DROP, o GRANT ALL PRIVILEGES.
3) Uso de consultas preparadas, en esta consulta se usan marcadores de posición. así la base de datos trata la inyección SQL como datos y no como un código ejecutable.

Conclusión

La identificación de las vulnerabilidades por explotación de una inyección SQL mediante DVWA nos ayuda a que tengamos actualizadas y seguras nuestras aplicaciones web.