Exploit

Victor Gerardo Rodríguez Barragán

29 de Octubre de 2023

1 SQL Injection

1.1 Descripción

La Inyección SQL es un tipo de ataque informático que permite a un atacante ejecutar comandos SQL maliciosos en una base de datos a través de una aplicación web. Estos comandos pueden manipular, filtrar o robar datos de la base de datos, y en algunos casos, pueden llevar a la eliminación de datos. Los atacantes pueden también utilizar este método para tomar el control de una aplicación web y, en última instancia, del servidor subyacente.

1.2 Descripción de la vulnerabilidad

La vulnerabilidad subyacente en un ataque de inyección SQL generalmente ocurre cuando una aplicación web no valida o escapa correctamente las entradas de usuario que se utilizan en las consultas SQL. Esto permite que los atacantes introduzcan comandos SQL en campos de entrada, que luego se ejecutan de manera inadvertida en la base de datos.

1.3 Caso de uso

El impacto de un ataque de Inyección SQL puede ser significativo. Los atacantes pueden acceder, modificar o eliminar datos confidenciales, como información de usuarios, contraseñas o registros financieros. También pueden comprometer la seguridad de la aplicación y el servidor subyacente, lo que podría permitirles tomar el control completo del sistema.

1.4 Como se lleva a cabo

La explotación de la Inyección SQL generalmente se realiza insertando comandos SQL maliciosos en los campos de entrada de una aplicación web, como formularios de búsqueda o campos de inicio de sesión. Si la aplicación no valida ni escapa adecuadamente estas entradas, los comandos se ejecutan directamente en la base de datos.

1.5 Herramientas

- **SQLMap:** Una herramienta automatizada que permite a los atacantes detectar y explotar vulnerabilidades de Inyección SQL en aplicaciones web.
- **Havij:** Una herramienta similar a SQLMap que automatiza la detección y explotación de Inyecciones SQL.
- **SQLMate:** Es una herramienta de prueba de penetración de código abierto que automatiza el proceso de detección y explotación de fallas de inyección SQL y toma el control de servidores de bases de datos. Viene con un potente motor de detección, muchas características de nicho para

la prueba de penetración y una amplia gama de interruptores que incluyen detección de huellas dactilares, enumeración de tablas, columnas, consultas, etc.

2 Referencias

- **https://www.imperva.com/learn/application-security/sql-injection-sqli/**
- **https://www.owasp.org/index.php/SQL_Injection**
- **https://www.acunetix.com/websitesecurity/sql-injection/**
- **https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/**
- **SQLMap: http://sqlmap.org/**
- **Havij: http://itsecteam.com/en/projects/project1.htm**