Brandon David Meza Vargas - 3CV11

SISTEMA DE DETECCIÓN DE INTRUSIONES EN APLICACIONES WEB PARA ATAQUES DE VALIDACIÓN DE ENTRADAS

APLICACIONES WEB COMO PRINCIPAL OBJETIVO DE ATAQUE

En USA más del 75% de los ataques son dirigidos a sitios web. Los ataques de validación de entradas pueden ocurrir cuando la información de peticiones web no es validada antes de ser usada por una aplicación web.

INPUT VALIDATION ATTACKS

Uno de los principales objetivos de los IVAs es tratar de enviar datos que la aplicación no pretende recibir. Estos ataques pueden ser categorizados segun sus metas

CATEGORIZACIÓN DE IVAS

- **Generar error de información:** el error revela direcciones de directorios o código fuente
- **Obtener acceso arbitrario a datos:** un usuario puede tener acceso a información importante o poder ver, crear o eliminar usuarios
- **Cross-Site Scripting:** se ejecutan comandos de sistema para vulnerar la aplicación

DEFENDAS COTNRA IVAS

Para protegernos de IVAs es importante tener una validación del lado del servidor, codificación de caracteres, expresiones regulares, fuerte tipado de datos, manejo apropiado de errores y usar autenticación

SISTEMA DE DETECCION DE INTRUSION EN APPS WEB CONSISTE EN 4 PASOS

1.COLECCIÓN DE DATOS

Recolección de parámetros en peticiones HTTP, cabeceros de peticiones GET y POST que usan parámetros para pasar valores a la aplicación.

2.EXTRACCIÓN DE PALABRAS CLAVE

Se extraen y se transforman valores importantes usando la matriz de reemplazo de palabras clave

3.MEDICIÓN DE SIMILITUD

Se mide la similitud de los datos en peticiones web, esto para encontrar la secuencia de peticiones web más común, usando la detección de la secuencia más optima

$$OSD^{*}(P,S) = \min_{0 \le KeyProDiff \le 1} \{OSD_{KeyProDiff}(P,S)\}$$

4.FILTRADO Y REPORTE

Filtra y reporta cuando las peticiones HTTP violan el estándar de una petición web normal

IMPLEMENTACIÓN

El sistema se realizo con Java y tiene 3 módulos

- **Módulo de recolección de datos:** Se implementa el paso 1 de la técnica
- **Modulo de análisis:** Se implementa el paso 2 y 3 de la técnica
- **Módulo de administración:** se implementa el paso 2 y 4 de la técnica