Validación de Entradas

Angel Martinez

angel.martinez@wizeline.com

Acerca de mí

Angel Martínez

Staff Software Engineer

- 8 años de experiencia
- 5 años en Wizeline
- Diseño de arquitectura y soluciones

Puntos importantes

Identifícate en Zoom utilizando tu nombre y apellido.

Mantén tu micrófono apagado durante el transcurso de la sesión.

Utiliza el chat para hacer tus preguntas durante la sección de Q&A.

Procura enfocar tus preguntas al tema presentado.

Apaga tu cámara en caso de tener problemas con tu conexión.

Código de conducta

Sé respetuoso, no hay malas preguntas o ideas.

Sé cordial y paciente.

Sé cuidadoso con tus palabras.

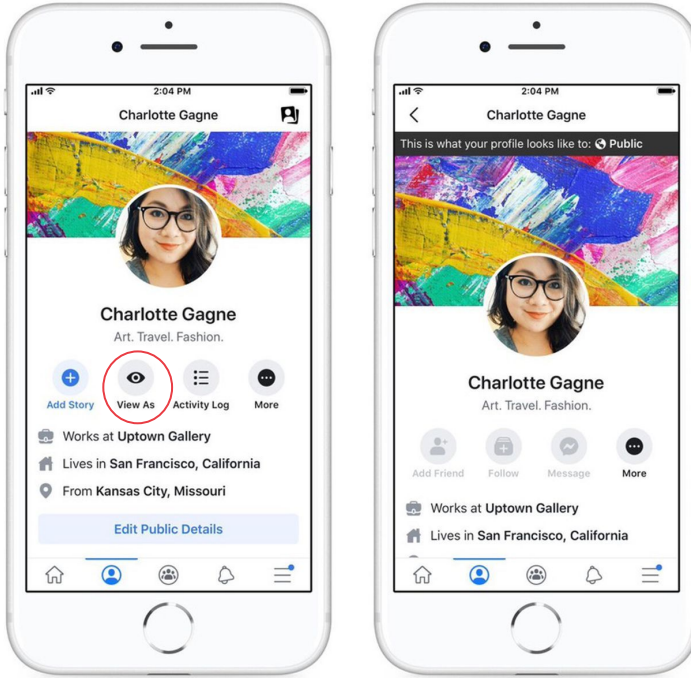
Objetivo

Al final de esta sesión podrás:

- Reconocer la importancia de la validación de entradas e identificar técnicas de prevención

Table de Contenidos

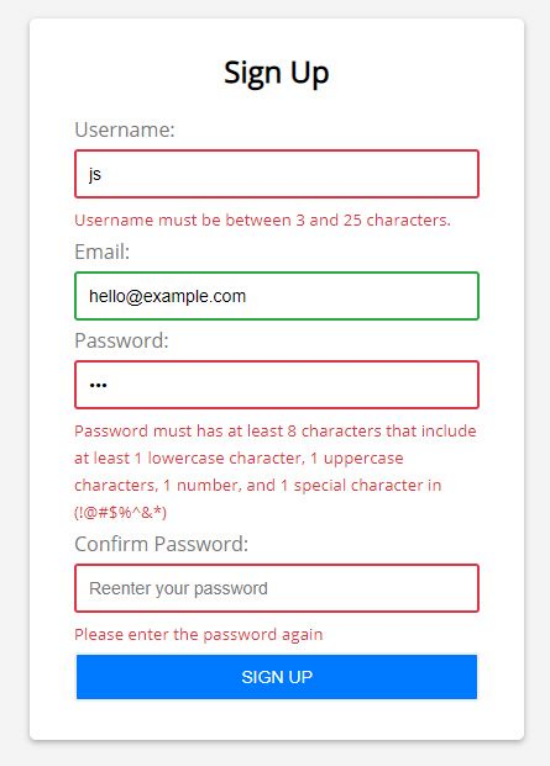
Introducción



En 2018, 50M users of Facebook fueron comprometidos por la vulnerabilidad **Ver como**

¿Qué es validación de entrada?

- Principio de código seguro
- **Validar y verificar** toda la información proporcionada al sistema
- **Recuerda: Nunca confíes en la información proporcionada por los usuarios**



Consecuencias

- Vulnerable a ataques de inyección
- Brechas de datos: Divulgación y robo de información sensible
- Acceso no autorizado
- Pérdida de reputación y confianza
- Acciones legales

Table de Contenidos

Importancia

Importancia

Seguridad

- Evita comprometer **integridad, confidencialidad y disponibilidad**

Prevención

- Protege contra ataques de:
  - SQL injection
  - XSS injection
  - Buffer overflow

Integridad

- Protege contra comportamientos no esperados, recibiendo solamente parámetros bien definidos

Importancia

Experiencia de Usuario

- Ayuda a manejar errores de manera proactiva, otorgando retroalimentación en tiempo real al usuario

Cumplimiento

- Garantiza el tratamiento de los datos, apegado a regulaciones y requerimientos

Validación Semántica

- Rangos numéricos
- Fechas
- Años
- Teléfonos
- Correos electrónicos
- Direcciones
- Longitud (Max-Min)
- Tipado
- Positivo/Negativo

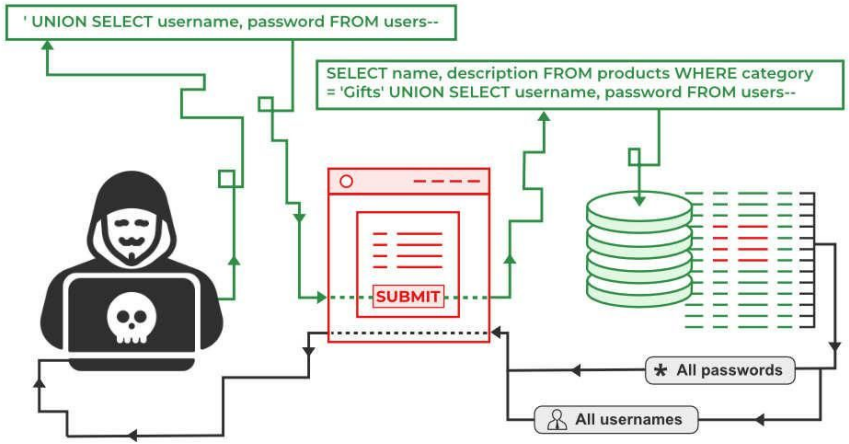
Table de Contenidos

Ataques Comunes

SQL injection

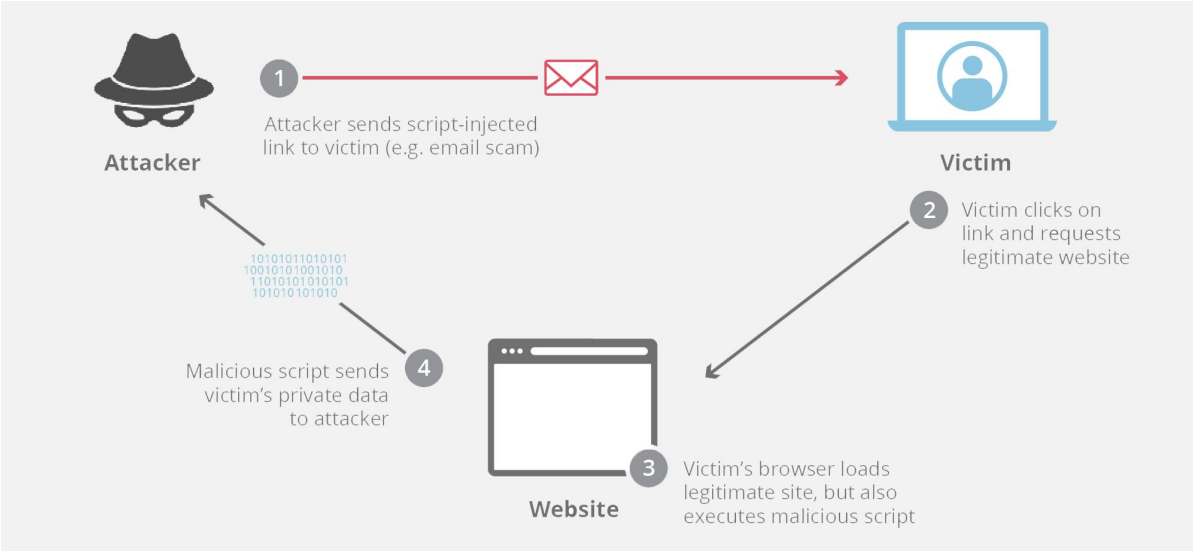
- Conversión de entradas a consultas SQL

```
SELECT * FROM users WHERE username='' AND password='' OR '1'='1';
```



XSS injection

- Cross-Site Scripting (XSS) inyección de código malicioso o scripts en la aplicación



Ejercicios

Almacenado (Persistente)

- El código malicioso se almacena en el servidor o en la base de datos

Reflejado

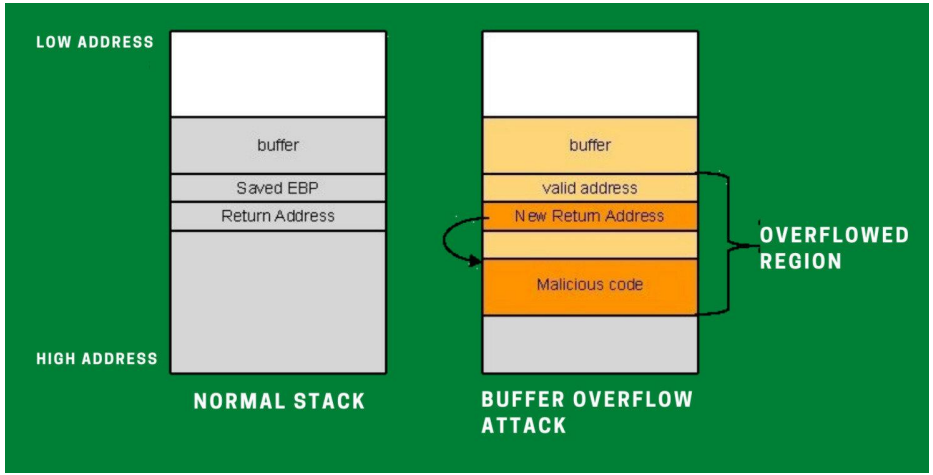
- El script malicioso proviene de la petición HTTP como lo son los parámetros de la URL

DOM-Based

- El código malicioso existe de lado del cliente

Buffer Overflow

- Procesamiento de datos más allá de los límites de memoria desbordando ubicaciones adyacentes.
- Provoca **fallos, ejecución arbitraria de código y escalación de privilegios**



Ejercicios

SQL Injection

- https://www.hacksplaining.com/exercises/xss-stored

XSS Injection

- https://www.hacksplaining.com/exercises/xss-stored

Buffer Overflow

- https://www.hacksplaining.com/exercises/buffer-overflows

Table de Contenidos

Técnicas de Prevención

Técnicas de prevención

Sanitización

- Limpieza y filtrado de entradas
- **Remover código malicioso, caracteres y símbolos especiales**
- Evitar trabajar con información no bien definida

Validación de Formato

- **Sintáctico**
  Sintaxis correcta para la estructura de los datos
- **Semántico**
  Alineados al contexto de negocio
  (Rangos, Longitudes, Fechas, Husos Horarios, Tipos)

Codificación

- Conversión de datos de manera segura para su la **transmisión, almacenamiento y visualización**

Técnicas de prevención

Listas (Allow/Block)

- Se rechaza por defecto y se acepta solo valores permitidos y viceversa

Regex

- Validación de formatos de datos mediante patrones previamente establecidos

Validación de Archivos

- Validación de **tamaños, tipos de archivos, rutas.**

Prevention Techniques

Validación (Cliente/Servidor)

- **Cliente:** Validar la información de antes de ser enviada al servidor, otorgando retroalimentación en tiempo real
- **Servidor:** Validar la información de antes de ser procesada o almacenada

Validación de Esquema

- Comparación de información proporcionada con las propiedades definidas en el esquema **(JSON, XML, Class, etc.)**

Herramientas

- Microsoft AntiXSS Library
- Data Annotations
- Fluent Validation Library

Table de Contenidos

Ejercicio de Código

Recapitulación

Hemos hablado acerca de:

- Introducción a la validación de entrada
- Importancia
- Ataques comunes
- Técnicas de prevención
- Implementación

¿Preguntas?

Retroalimentación

Déjanos saber tu retroalimentación

Gracias.