THE BRIDGE

CYBER SECURITY

Cross Site Scripting

Cross Site Scripting (XSS)

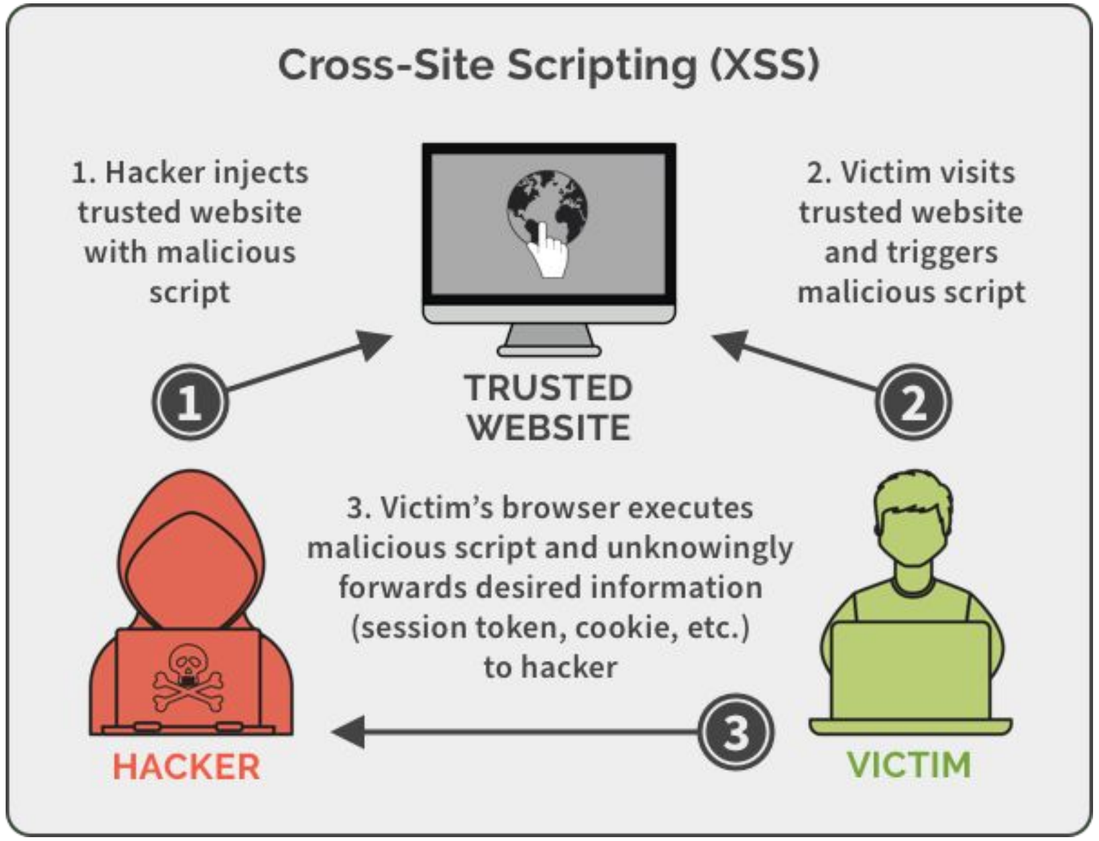
- El **Cross Site Scripting o XSS** es un tipo de ciberataque por el cual se buscan vulnerabilidades en una aplicación web para **introducir un script dañino** y atacar su propio sistema, partiendo de un contexto fiable para el usuario.

- Los scripts son archivos de comandos o programas escritos en lenguajes de programación –como **JavaScript**– que se ejecutan en el navegador web.

- En su versión más inocua se ejecutan ventanas emergentes y, en el peor de los casos, son utilizados por atacantes para acceder a información sensible o al equipo del usuario.

- Siempre que una aplicación web transfiera datos de usuario no validados al navegador.

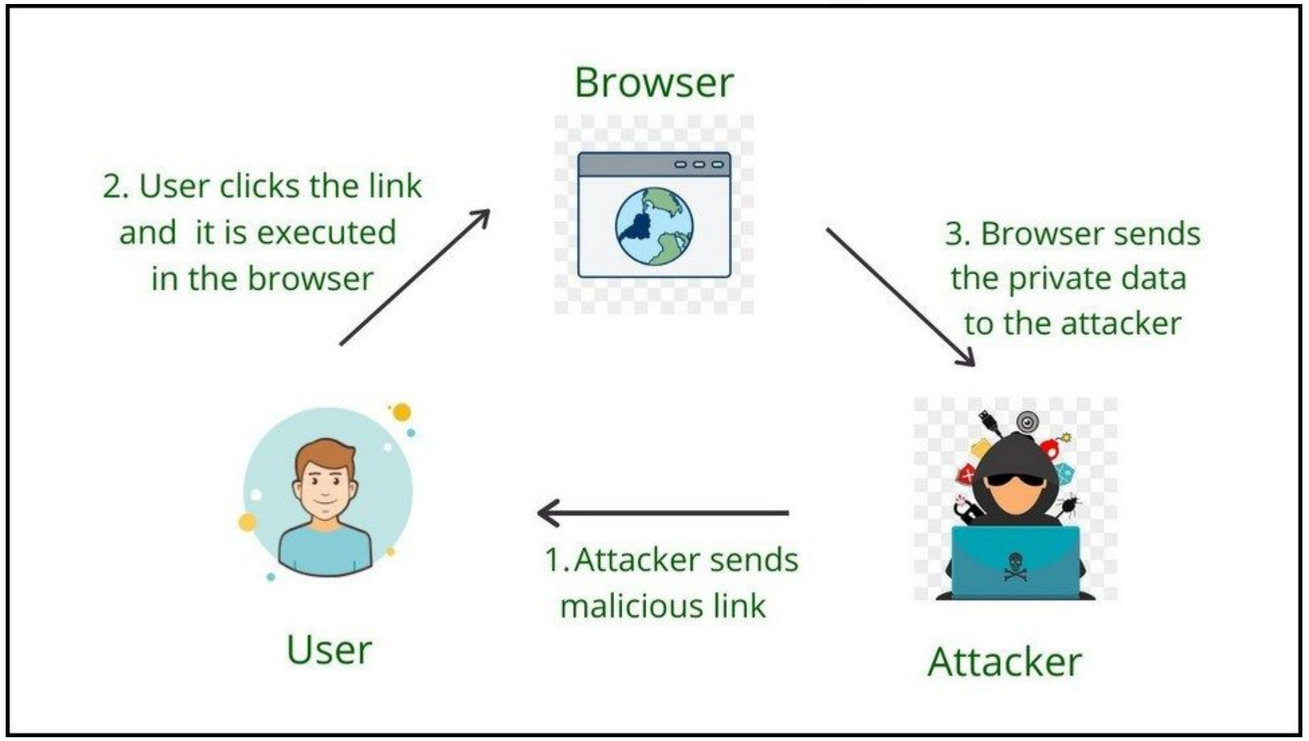
- Las aplicaciones infectadas manipulan scripts propios de la página tales como formularios de registro y, mientras que para el usuario todo indica que se trata de una página protegida, en realidad los datos están siendo transferidos a otro sitio sin ningún tipo de filtro.



https://blog.hubspot.com/website/cross-site-scripting

Tipos de XSS

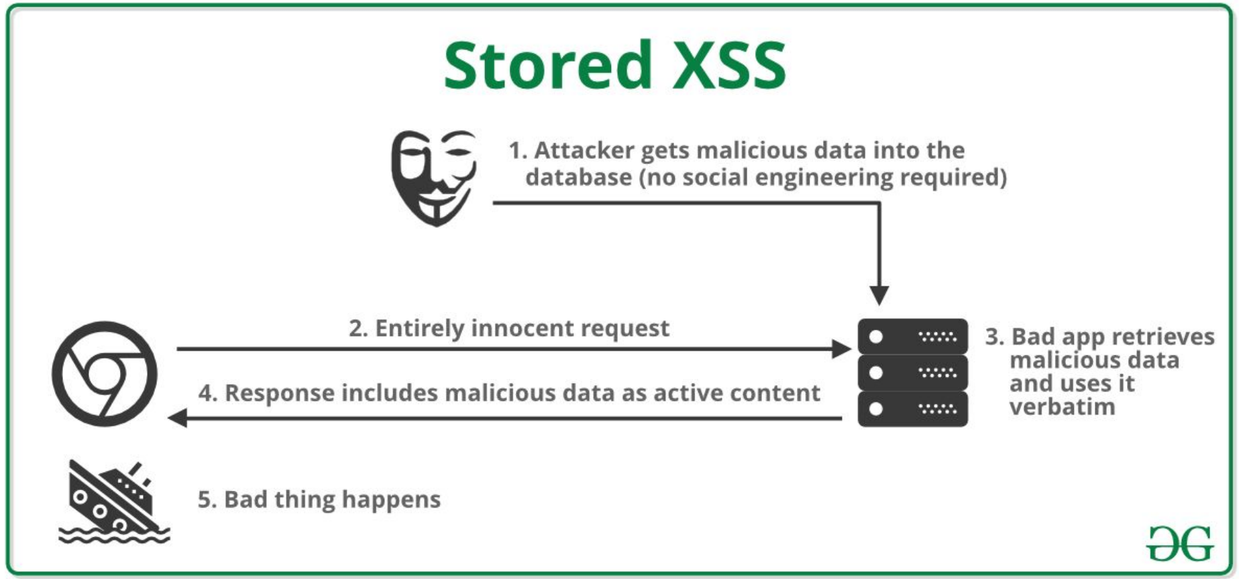
- **Reflected Cross-Site Scripting**
  - Los ataques **non-persistent XSS** o **reflected XSS**, no almacenan el código malicioso en el servidor, sino que lo pasan y presentan directamente a la víctima.
  - Es el método más popular de ataque **XSS**.
  - El ataque se lanza desde una fuente externa, mediante email o un sitio de terceros.
  - Las páginas **webs dinámicas** y las **aplicaciones de correo** son más vulnerables.
  - Ejemplo :
    - **http://tubancoonline.com/index.php?user=&script>código_malicioso</script>**



https://www.geeksforgeeks.org/reflected-xss-vulnerability-in-depth/

Tipos de XSS

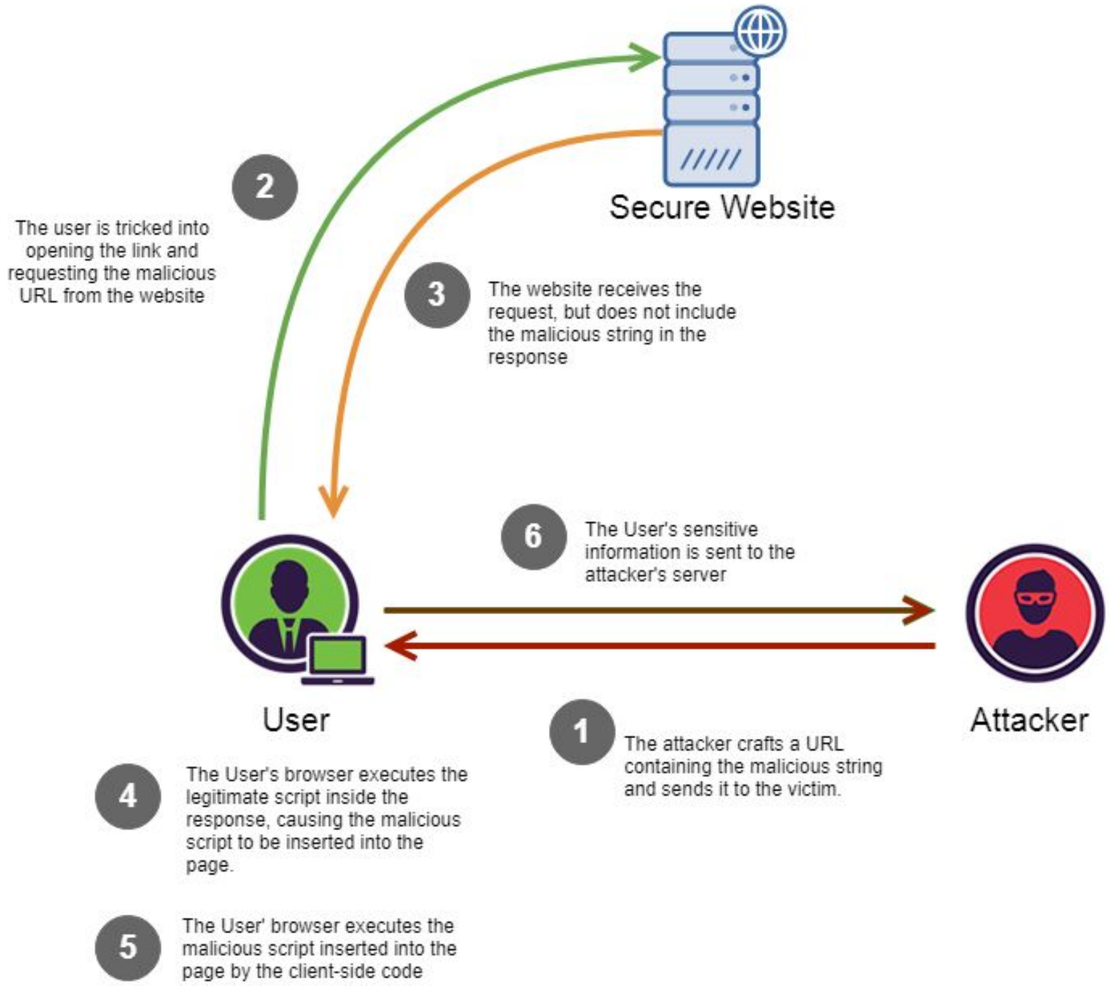
- **Stored Cross-Site Scripting**
  - El código malicioso ya ha superado la barrera del proceso de validación y está almacenado en un servidor.
  - Usado en aplicaciones web que guardan datos de usuario en su propio servidor y los transfieren sin métodos de control o codificación
  - Puede ser un comentario, un archivo log, un mensaje de notificación, o cualquier otro tipo de sección del sitio web que solicita algún input al usuario.
  - Cuando la información se presenta en el sitio web, el código malicioso es ejecutado.
  - Los blogs y los foros son especialmente vulnerables para este tipo de ataques
  - Ejemplo de post :
    - **”Hola mi nombre es Pepe y estoy buscando <script>código malicioso</script>”**



https://www.geeksforgeeks.org/what-is-cross-site-scripting-xss/

Tipos de XSS

- **DOM-based Cross-Site Scripting**
  - También llamado **XSS local**, en este caso el daño se provoca por medio de los scripts que están en el lado del cliente.
  - Al abrir una página infectada, el código malicioso puede aprovechar un agujero en la seguridad para instalarse en un archivo del explorador web y ser ejecutado allí sin ninguna comprobación previa.
  - En este caso el servidor web no está implicado, por lo que este ataque también afecta a las páginas estáticas que implementan este tipo de lenguaje de programación
  - **Ejemplo:**
    - ”Como **el XSS reflejado**, el Cross Site Scripting basado en **DOM** requiere que el usuario abra el enlace.
    - Cuando esto sucede, un script de la página web selecciona la variable de la URL y ejecuta el código que contiene.
    - Es así como se pueden usurpar **cookies** de sesión, entre otras cosas”



https://medium.com/iocscan/dom-based-cross-site-scripting-dom-xss-3396453364fd


THE
BRIDGE