1.Cross-Site Scripting

É uma vulnerabilidade encontrada nos aplicativos da Web. **XSS permite que os criminosos injetem scripts contendo código malicioso em páginas Web**. O script entre o site tem três participantes: o criminoso, a vítima e o site. O criminosos virtual não mira diretamente na vítima. O criminoso explora a vulnerabilidade dentro de um site ou aplicativo da Web. Os criminosos injetam scripts no cliente em páginas Web visualizadas pelos usuários. O script mal-intencionado inadvertidamente passa para o navegador do usuário. Se obtiver o cookie de sessão da vítima, os criminosos poderão se passar pelo usuário.

Os ataques XSS exploram a confiança do navegador da vítima, que executa o código malicioso como se fosse parte legítima da página. Os ataques XSS também podem ser usados para roubar informações confidenciais, como cookies de sessão, ou para redirecionar os usuários para sites maliciosos.

2.Tipos de XSS

Há três tipos principais de XSS:

2.1 Refletido (Reflected XSS)

Neste tipo, o código malicioso é incorporado em um link ou em um campo de entrada, e a vítima é enganada para clicar no link ou acessar uma URL específica que contenha o código. O servidor web reflete o código de volta para a vítima, que o executa.

2.2 Armazenado (Stored XSS)

Neste caso, o código malicioso é armazenado no servidor, geralmente em um banco de dados, e é exibido para os usuários sempre que uma página específica é acessada. Comentários de fóruns ou campos de perfil em redes sociais são alvos comuns de ataques de XSS armazenados.

2.3 DOM-based (DOM-based XSS)

Esse tipo de XSS ocorre no lado do cliente, quando o código malicioso manipula o ***Document Object Model*** (DOM) da página web após o carregamento, sem necessariamente modificar o conteúdo no servidor. É mais difícil de detectar e mitigar, pois o código malicioso não viaja para o servidor.

3.Prevenção e mitigação de XSS

A prevenção e a mitigação de Cross-Site Scripting (XSS) são fundamentais para proteger aplicativos web contra essa vulnerabilidade comum. Isto significa que os esforços devem ser contínuos, pois as ameaças e as técnicas de ataque evoluem constantemente. Manter-se atualizado sobre as melhores práticas de segurança e monitorar seu aplicativo regularmente é essencial para proteger seus sistemas e os dados dos usuários contra ataques XSS de maneira eficaz.