Домашнее задание №6

1. Этому примеру кода соответствует потенциальная уязвимость XSS (Cross-Site Scripting).

   CWE-79: Improper Neutralization of Input During Web Page Generation.

   <script>alert('XSS')</script>), если кто то введет данный скрипт, он будет выполнен в браузере других пользователей, открывающих страницу.
   Для решения уязвимости нужно экранировать ввод htmlspecialchars.

2. CWE-284: Improper Access Control описывает уязвимости, связанные с недостатками в реализации или применении механизмов контроля доступа. Это позволяет злоумышленникам получить доступ к ресурсам или выполнить действия, которые должны быть запрещены, например, доступ к данным, изменение настроек или выполнение операций от имени другого пользователя.

3. 22 октября 2024 г. Агентство кибербезопасности и безопасности инфраструктуры (CISA) опубликовало предупреждение об использовании критической уязвимости, затрагивающей Microsoft SharePoint. Эта уязвимость, обозначенная как CVE-2024-38094, представляет собой уязвимость десериализации, которая делает возможным удаленное выполнение кода (RCE). Эта уязвимость может позволить злоумышленнику получить контроль над необновленными системами SharePoint, ставя под угрозу безопасность организаций. Эта уязвимость затрагивает экземпляры Microsoft SharePoint, где ненадежные данные могут быть десериализованы, создавая вектор атаки для удаленного выполнения кода. Это позволяет злоумышленнику отправлять вредоносные данные, вызывающие непредвиденное поведение приложения.