Задание выполнил студент группы 2345 Романенко Кирилл

1. Внимательно изучите все задачи из раздела «Практика» данной методички и ответьте: как можно использовать поисковые запросы при поиске уязвимостей XSS?

   1. Поиск общих полезных нагрузок XSS, таких как "<script>alert('XSS')</script>" и "<img src=x onerror=alert('XSS')>".
   2. Поиск HTML-тегов, которые могут быть использованы для внедрения вредоносного кода, таких как <iframe>, <script>, <img>, <a> и т.д.
   3. Поиск полей пользовательского ввода, таких как текстовые поля и поля поиска, которые могут быть уязвимы для атак XSS.
   4. Поиск параметров URL, которые могут быть уязвимы для XSS-атак.
   5. Поиск функций JavaScript, которые могут быть уязвимы для XSS-атак, такие как eval(), setTimeout() и setInterval().

2. Допустим, вы обнаружили, что на странице есть уязвимый к XSS параметр, в который можно выполнить инъекцию вектором `<script>alert(document.cookie)</script>`. Как проверить, к какому типу относится инъекция (Reflected, Stored, DOM, Self или Blind)? Ответ обоснуйте.

   <script>(document.cookie)</script> - пример Reflected XSS.

   Reflected XSS, в частности, происходят, когда внедренный скрипт отражается обратно пользователю в ответе веб-приложения.

   В этом случае внедренный скрипт будет выполнен, когда веб-приложение отобразит его обратно в браузере пользователя, отобразив окно предупреждения, содержащее информацию о файлах cookie пользователя. Эта атака часто используется злоумышленниками для кражи сессионных файлов cookie, что позволяет им выдавать себя за пользователя и получать доступ к конфиденциальной информации.

   Чтобы подтвердить, что внедренный скрипт является примером Reflected XSS, нужно изучить, как внедряется и выполняется скрипт. Если скрипт

хранится в базе данных приложения и выполняется всякий раз, когда пользователь обращается к определенной странице, то это будет рассматриваться как Stored XSS.
Однако в данном случае скрипт вводится в URL веб-приложения и отражается обратно пользователю в ответе. Это подтверждает, что атака является примером Reflected XSS.