Задание 4.

1) Уязвимость: stored XSS HTML контекст

Шаги: 1) Записать XSS в строку “Расскажите о ваших впечатлениях”

2) Добавить через нажатие кнопки “Обзор…” картинку

3) Нажать кнопку “Отправить”

Запросы: <img src=x onerror=alert(23)>

2) Уязвимость: stored XSS: атрибут контекст

Шаги: 1) Записать XSS в строку “Расскажите о ваших впечатлениях”

2) Добавить через нажатие кнопки “Обзор…” картинку

3) Нажать кнопку “Отправить”

Запросы: <img src=x onmouseover=alert(1)>

3) XSS через комментарии с текстовыми ссылками

Шаги: 1) Записать XSS в строку “Расскажите о ваших впечатлениях”

2) Добавить через нажатие кнопки “Обзор…” картинку

3) Нажать кнопку “Отправить”

Запросы: Кликни здесь

4) Прямое добавление SVG на страницу

Шаги: 1) Записать XSS в строку “Расскажите о ваших впечатлениях”

2) Добавить через нажатие кнопки “Обзор…” картинку

3) Нажать кнопку “Отправить”

Запросы:

<svg xmlns="http://www.w3.org/2000/svg" onload="alert('777')"> <circle cx="50" cy="50" r="40" stroke="black" stroke-width="3" fill="red" /> </svg>

5) Уязвимость: stored XSS в имени пользователя

Шаги: 1) Написать комментарий

2) Добавить через нажатие кнопки “Обзор…” картинку

3) Нажать кнопку “Отправить”

4) В перехваченном запросе дешифровать часть токена, где зашито имя пользователя

5) Изменить эту часть на вредоносный скрипт, представленный ниже

6) Завершить отправку перехваченного запроса

Запросы: <script>alert('67896')</script>

6)