

Решение СЗИ-11 Защити лаунчер от хакеров

Описание

"Хакеры взломали редирект после входа в лаунчер Minecraft. Почини функцию редиректа так, чтобы хакеры не могли украсть аккаунты игроков."

Решение

Анализ уязвимости

Открываем задание и видим функцию `render_after_login()`, которая напрямую вставляет параметр `next_page` в JavaScript без валидации:

```
def render_after_login(next_page: str) -> str:
    # БЛОК ДЛЯ РЕДАКТИРОВАНИЯ:
    html = f"""
    <html>
        <head><title>Minecraft Launcher - Login Success</title></head>
        <body>
            <h1>Добро пожаловать!</h1>
            <p>Вы успешно вошли в лаунчер Minecraft.</p>
            <script>
                const next = "{next_page}";
                document.body.innerHTML += '<a href="' + next + '">Перейти
дальше</a>';
            </script>
        </body>
    </html>
    """
    return html
    # КОНЕЦ БЛОКА ДЛЯ РЕДАКТИРОВАНИЯ
```

Проблема: злоумышленник может внедрить JavaScript через параметр `next_page`, используя `javascript:` протокол или закрывая строку.

Пример решения

Добавляем whitelist валидацию и безопасное создание DOM элементов:

```
def render_after_login(next_page: str) -> str:
    allowed_pages = {'/servers'}

    if not next_page or not next_page.startswith('/'):
        safe_next = '/servers'
    elif next_page in allowed_pages:
        safe_next = next_page
    else:
        safe_next = '/servers'

    html = f"""
    <html>
      <head><title>Minecraft Launcher - Login Success</title></head>
      <body>
        <h1>Добро пожаловать!</h1>
        <p>Вы успешно вошли в лаунчер Minecraft.</p>
        <script>
          const next = "{safe_next}";
          const link = document.createElement('a');
          link.href = next;
          link.textContent = 'Перейти дальше';
          document.body.appendChild(link);
        </script>
      </body>
    </html>
    """
    return html
```

Получение флага

После отправки исправленного кода на проверку получаем флаг:

```
vsosh{d0m_b4s3d_xss_pr0t3ct10n_l4unch3r}
```