На сайте http://192.168.56.11/mutillidae/index.php?page=set-backgroundcolor.php отсутствует фильтр данных в форме для их ввода. Это позволяет выполнить XSS-инъекцию в исполняемом HTML-контексте.

Где найдена уязвимость

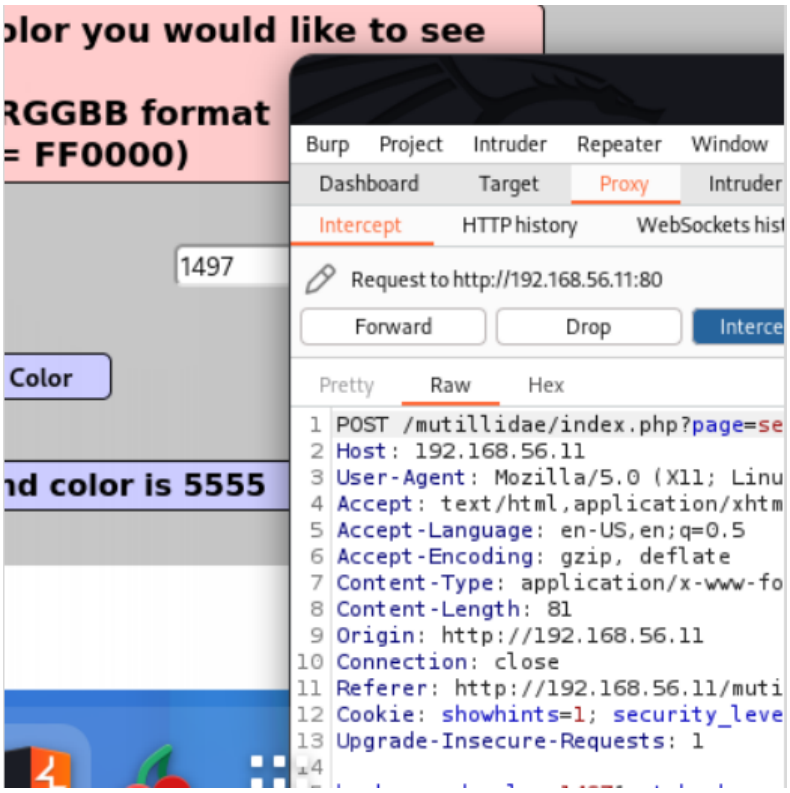
Уязвимость расположена по адресу http://192.168.56.11/mutillidae/index.php?page=set-background-color.php

Наименование продукта: Metasploitable 3 Linux virtual machine.

Технические детали обнаружения и воспроизведения

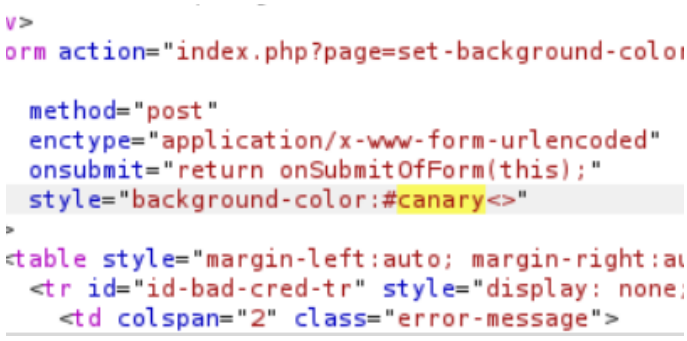
Уязвимость можно обнаружить на странице http://192.168.56.11/mutillidae/index.php?page=set-background-color.php

Ввела в форму ввода 1494 и перехватила запрос в Burp Suite:



При анализе запроса-ответа обнаружила, что введенные данные падают в тег style

Проверила наличие фильтрации. Её нет.

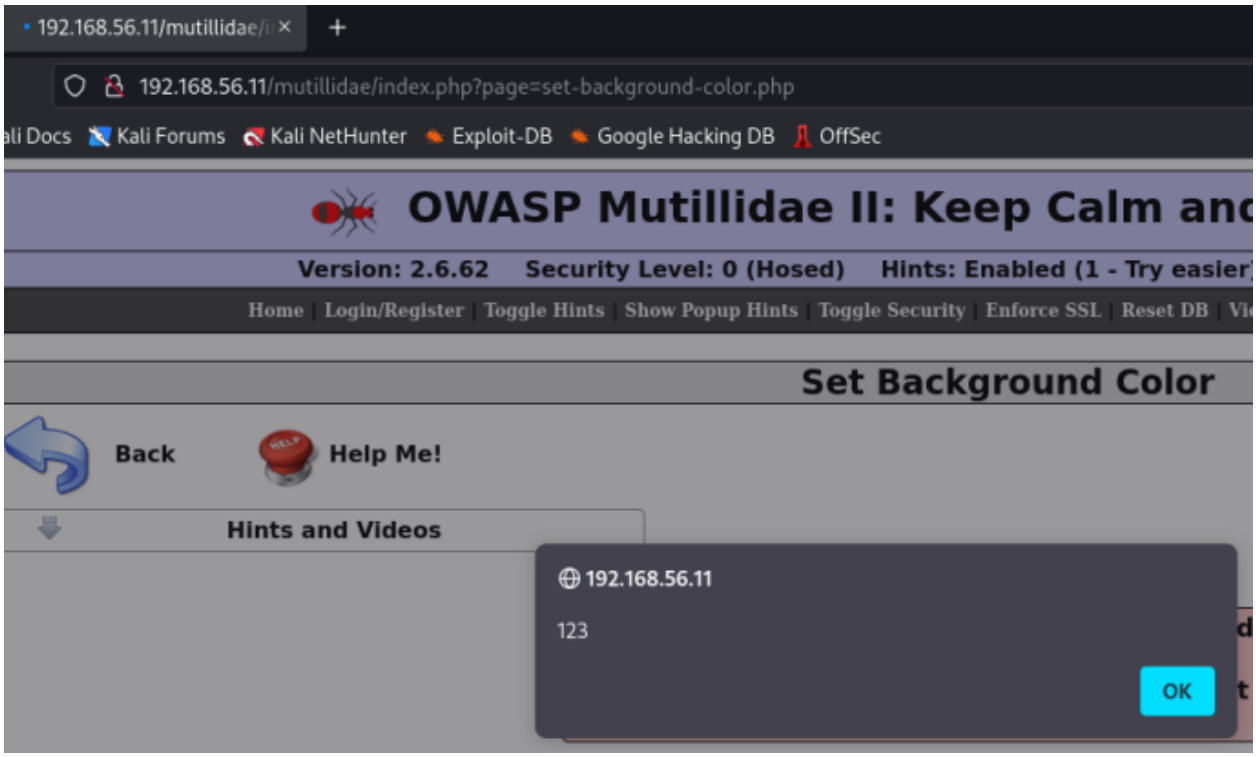


Ввела <script>alert(123)</script> в форму из двух точек срабатывания выбрала ту, которая проще.

1.
```
    onsubmit="return onSubmitOfForm(this);"
    style="
background-color:#<script>alert(123)</script>"
  >
  <table style="margin-left:auto; margin-right:autc
```

2.
```
informative-message" colspan="2" style="text-align:
center;">
095         The current background color is <script>alert(
123)</script>     </td>
096     </tr>
```

Открыла в Response in browser



Выводы и рекомендации по устранению

Уязвимость позволяет ввести исполняемый код в поле ввода. Не требует дополнительных уязвимостей для эксплуатации. Рекомендации по устранению:

- Запретить теги в пользовательском виде

- Запретить спец. символы

- Настроить CSP