

Задание выполнил студент группы 2345 Романенко Кирилл

1. Найдите XSS на странице Set Background Color проекта Mutillidae, составьте отчет о найденной уязвимости.

На сайте <http://192.168.56.11/mutillidae/index.php?page=set-background-color.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>

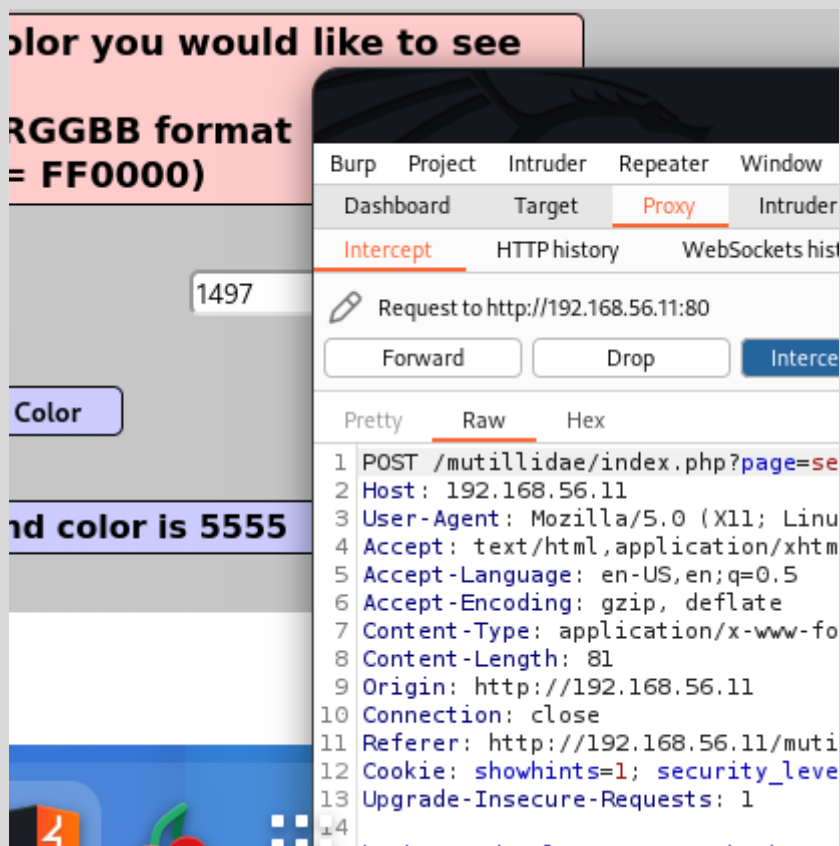
Наименование продукта: Metasploitable 3 Linux virtual machine.

Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить на странице

<http://192.168.56.11/mutillidae/index.php?page=set-background-color.php>

Ввел в форму ввода 1494 и перехватил запрос в Burp Suite:



При анализе запроса-ответа обнаружил, что введенные данные падают в `<div style`

Проверил наличие фильтрации. Её нет

```
v>  
form action="index.php?page=set-background-color.php"  
  
method="post"  
enctype="application/x-www-form-urlencoded"  
onsubmit="return onSubmitOfForm(this);"  
style="background-color:#canary<>"  
>  
<table style="margin-left:auto; margin-right:auto;">  
  <tr id="id-bad-cred-tr" style="display: none;">  
    <td colspan="2" class="error-message">
```

Ввёл `<script>alert(123)</script>` в форму

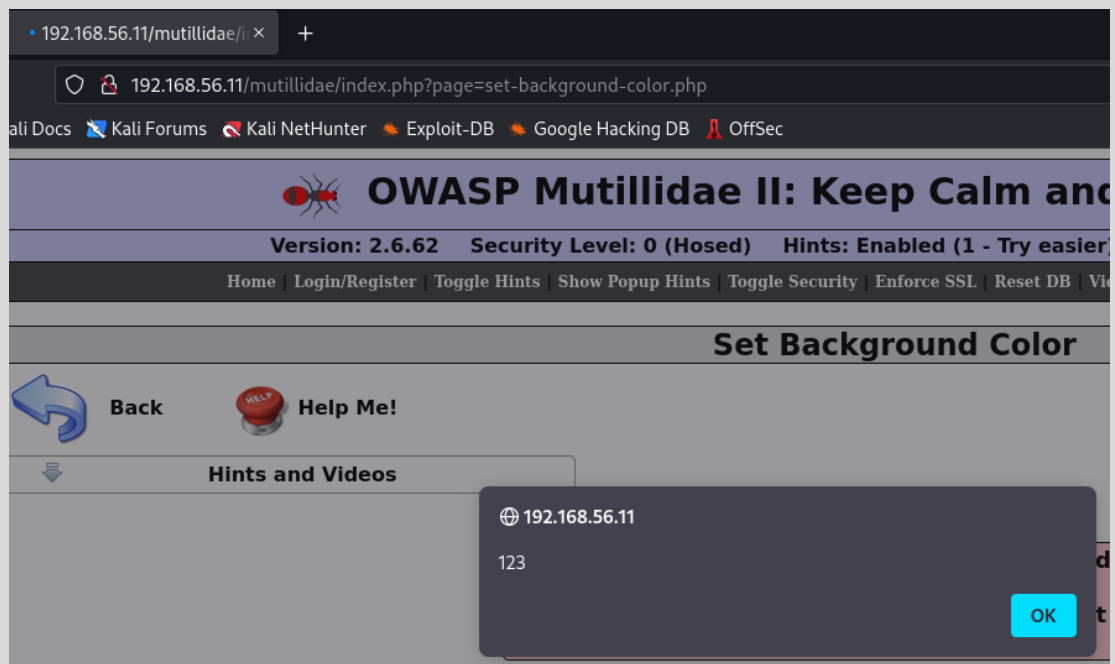
Из двух точек срабатывания выбрал ту, которая проще, т.е. № 2:

1.

```
55     onsubmit="return onSubmitOfForm(this);"  
56     style="background-color:#<script>alert(123)</script>"  
57   >  
58   <table style="margin-left:auto; margin-right:auto;">
```
2.

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

Открыл 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

Используемое программное обеспечение

- BurpSuite.
- FireFox Extended Support Release 102.5.0esr (64-bit).