In partial fulfillment of the requirement for
Cybersecurity
420-950-VA section 05811
Vanier College

osCommerce 2.3.4.1

Vulnerability Assessment

Professor:

Moustafa Mahmoud

Team members:

Chi-tao Li

Gerasimos Vlassopoulos

Md Ibrahim Ullah

Mark Benedict Muyot

Date of Submission:
February 05, 2023

TABLE OF CONTENTS

1. EXECUTIVE OVERVIEW

The group performed a vulnerability assessment on osCommerce V 2.3.4.1, the steps taken include reconnaissance, vulnerability detection, and exploitation. During reconnaissance, the target website was scanned for interesting end-points and a directory search tool was used. During vulnerability detection, various techniques were used including default credentials, brute-force attack, and searching for public CVEs. The test found two critical vulnerabilities: website hijacking and remote command execution. The website hijacking vulnerability is caused by the presence of an accessible /install folder that allows an attacker to reinstall the database, wiping out all stored data and potentially gaining administrative access. The remote command execution vulnerability is caused by a lack of proper input validation in the login.php script. Both vulnerabilities can be mitigated by keeping the osCommerce software up-to-date and implementing proper security measures.

Our team was able to apply all the learnings from Cybersecurity class. The group was also able to use some tools like Nmap, kali Linux, and dirsearch. A detailed report will be seen through this document on how to mitigate the vulnerabilities the team found on this web application.

2. OSCOMMERCE

2.1 What is osCommerce?

osCommerce (Open-Source Commerce) is an open-source e-commerce platform that allows users to create and manage an online store. Since its first release in 2000, it has grown to rank among the most widely used open-source e-commerce systems.

This web application became perhaps the most popular Ecommerce platform for a while. Unfortunately, because of the lack of the commercial strategy, osCommerce version 2 never took off as a successful viable commercial product, ready to support bigger businesses and help them with their challenges.

osCommerce is written in PHP and uses a MySQL database to store data. It is designed to be easy to use, customize, and integrate with other systems. It has a large community of users and developers who contribute to the platform by creating add-ons, modules, and themes. Some of the features include:

- Product management
- Order management
- Customer management
- Payment and shipping integration
- Multi-language support
- SEO optimization

.

2.2 Why the group chose osCommerce version 2.3.4.1?

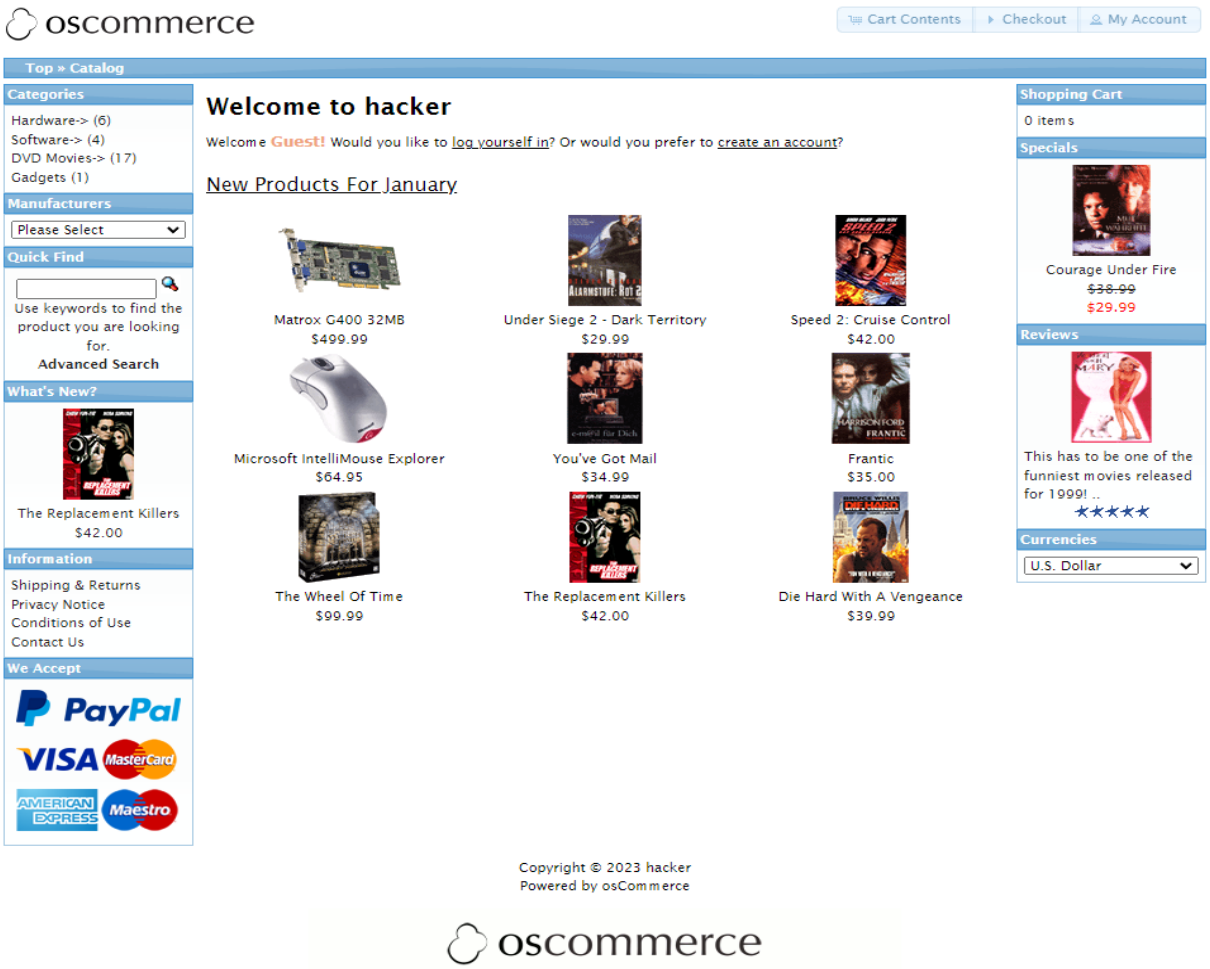
osCommerce ver 2 was released in June 2012 and had gained popularity since its first release. Currently, there are 46,000 shops using osCommerce. The popularity of this web application makes it a valuable target for pentesting because it is widely used by small to medium-sized online stores, and as such, it may contain vulnerabilities that could be exploited by attackers.

The group chose an older version of osCommerce, version 2.3.4.1, despite the latest version (osCommerce 4) being released on July 25, 2022. This decision was made because, as new pentesters, the group believed that the older version would have more vulnerabilities and therefore would be easier to exploit and apply all the lessons learned from this subject. The web app was downloaded from this website, https://phpsources.net/script/php/ecommerce/2022-1_oscommerce,2.3.4.1.

Additionally, osCommerce being open-source software allowed the group to easily access the source code and perform a deep dive in the platform, this way, it is easier to spot vulnerabilities in relation to OWASP top 10 and test them.

3. RECONAISSANCE

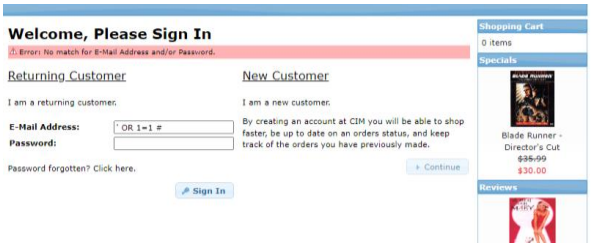
Our target looks like this:

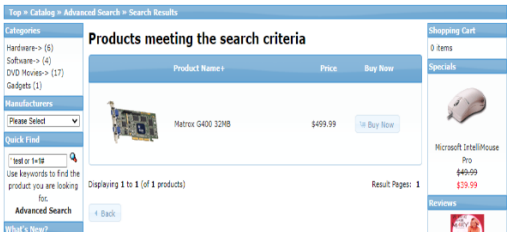


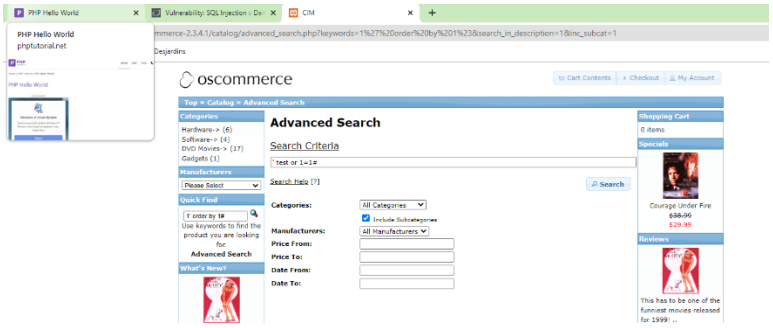
The team searched and gathered as much information about osCommerce before proceeding to the next step. We even checked for existing exploits done in this website through www.cvedetails.com

As part of our reconnaissance, the team also tested some possible attack vectors to check for vulnerabilities.

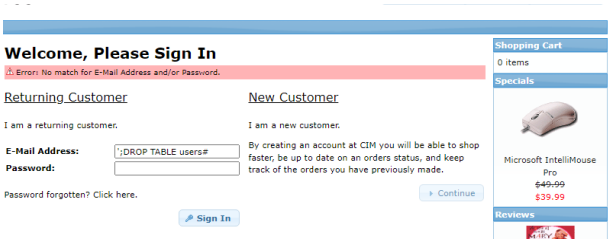
Tautology attacks on login, search criteria and advanced search page

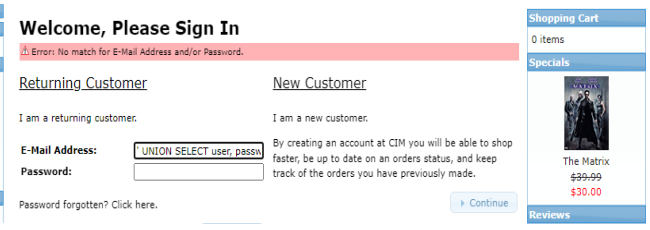


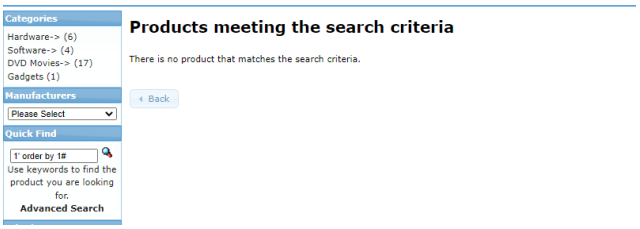




The team also performed union, piggy backed attack and etc. on certain attack vectors.



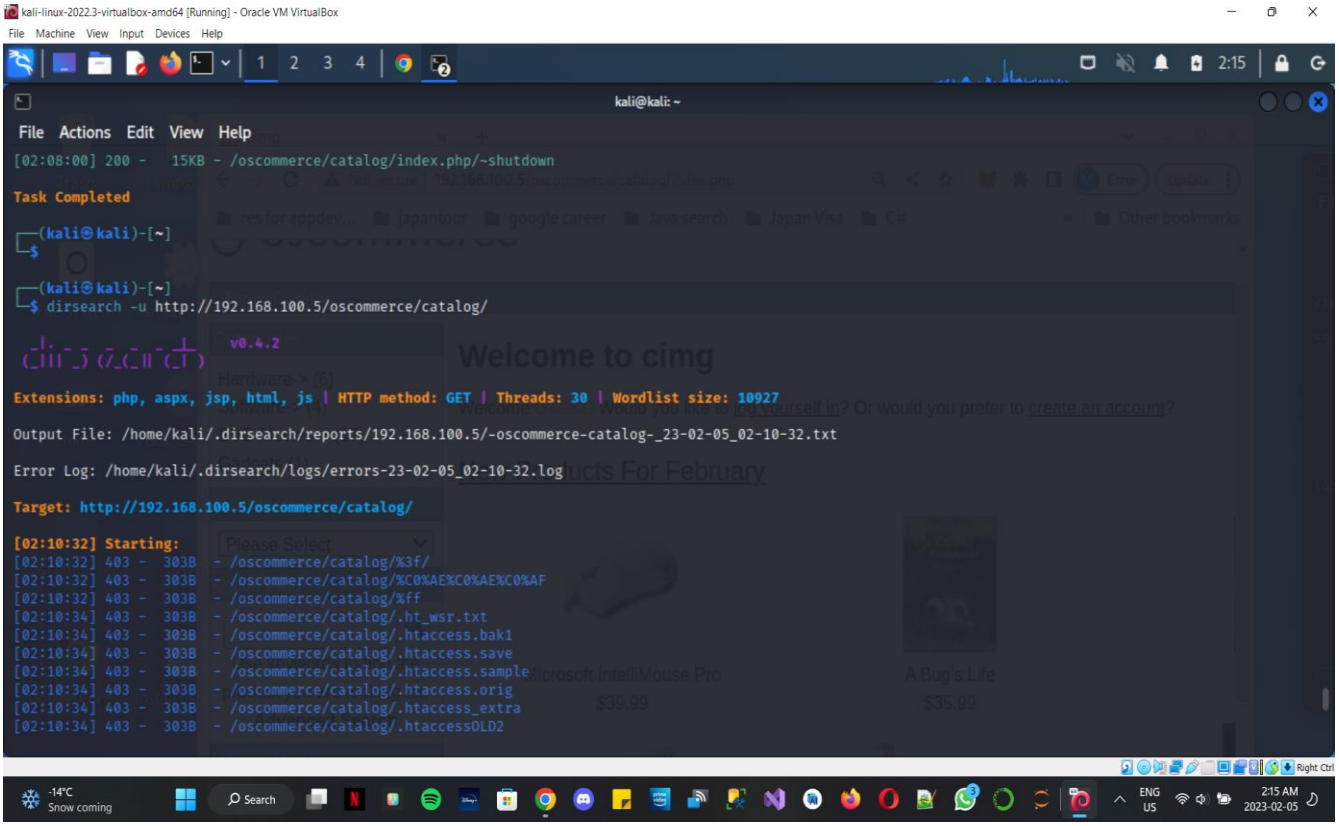


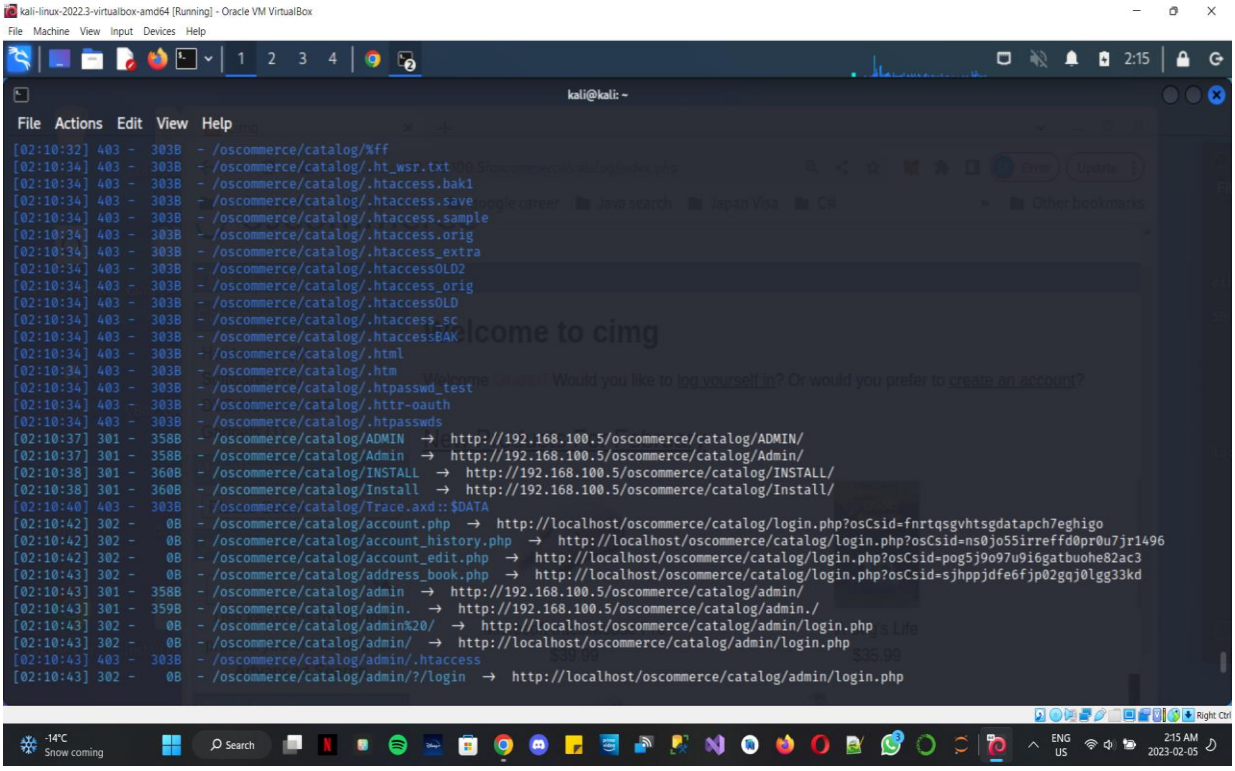


4. SCANNING

Our team used a dirseach. A tool that will show us the different endpoints that we can access in this website.

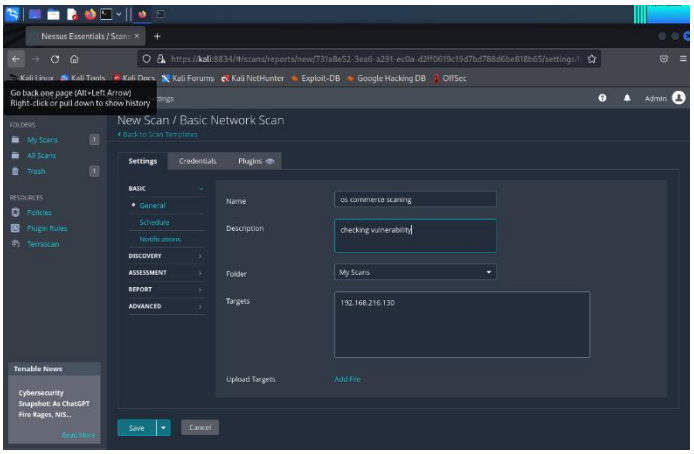
Command used: dirsearch -u http://192.168.100.5/oscommerce/catalog

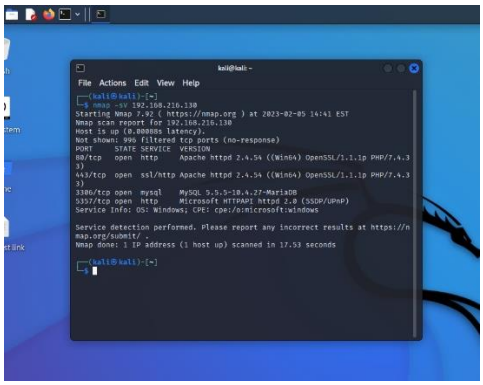




The command showed us all directories and end-points we can access and the team tried exploiting install page and login page.

A Nessus and Nmap Scan was also done:

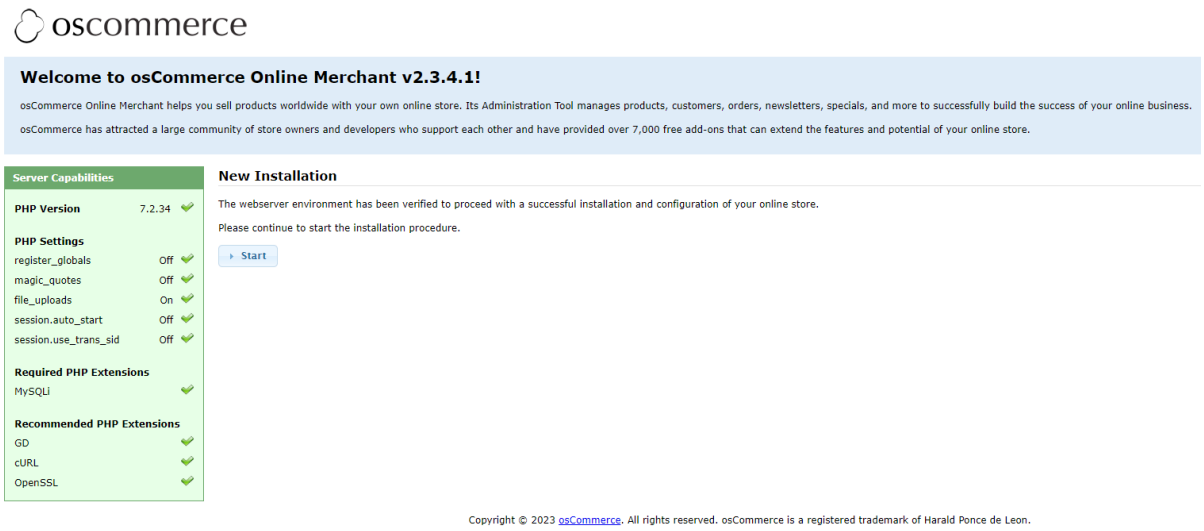




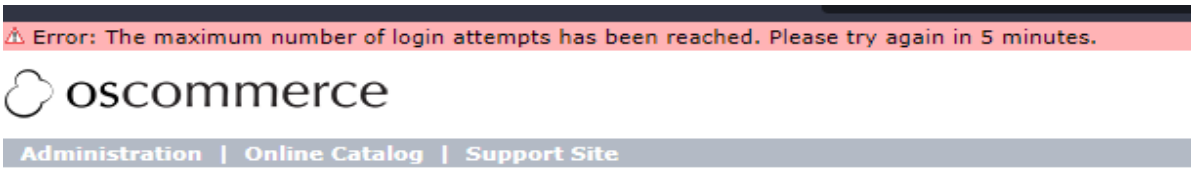
5. VULNERABILITY DETECTION

The team used various techniques for vulnerability detection including default credentials, brute-force attack, and searching for public Common Vulnerabilities and Exposures (CVEs). The team examined the website and try to perform SQLI in all possible attack vectors in the application.

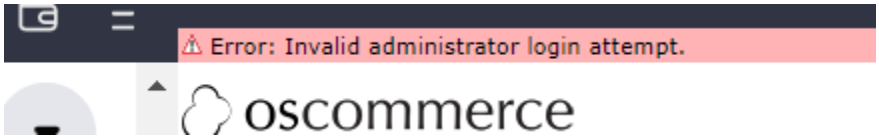
Install Page



Login page



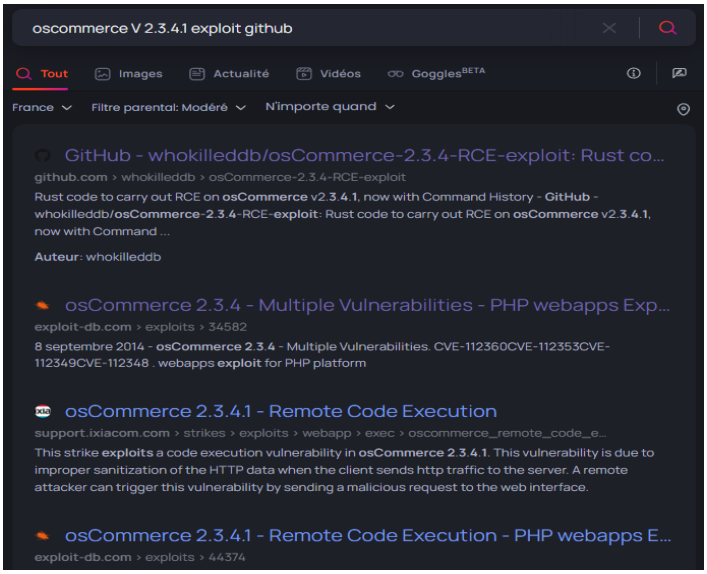
One of the tricks we can check is default credentials like



Login was tried to be exploited also but this web app implemented a delay every time you reach a maximum attempt on a particular username. We even tried to check default credentials by entering **admin/admin** or **admin/123456** or **admin/password** in the username and password but we were not able to detect any vulnerabilities in this page.

In our opinion, Brute force attack wont work in this web app. Perhaps a spray attack will work if you are able to access this website.

Since basic checks did not lead us to any interesting result, we searched for public CVE affecting this **osCommerce V 2.3.4.1**

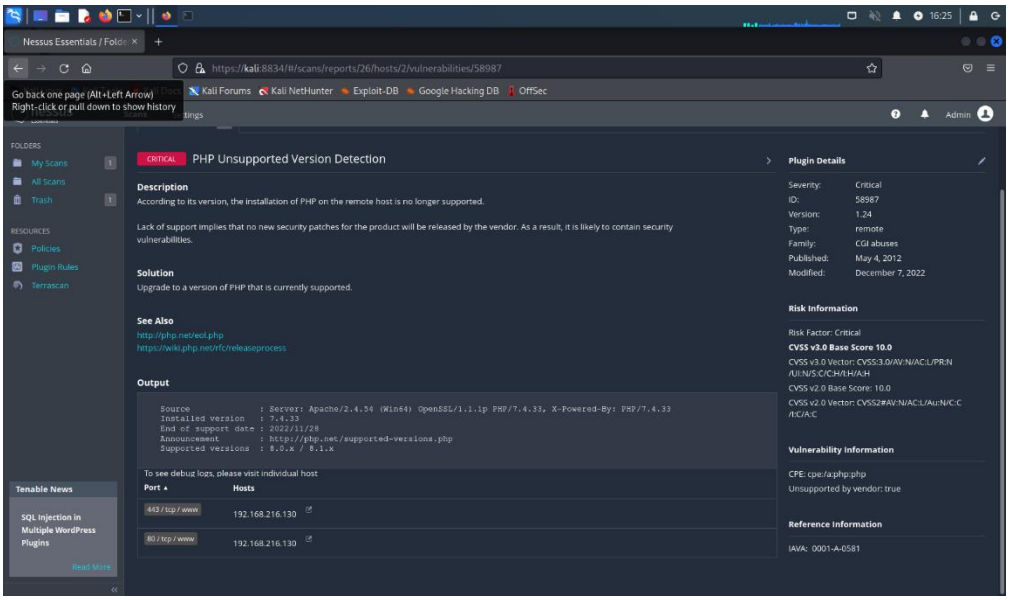


The following critical vulnerabilities were identified:

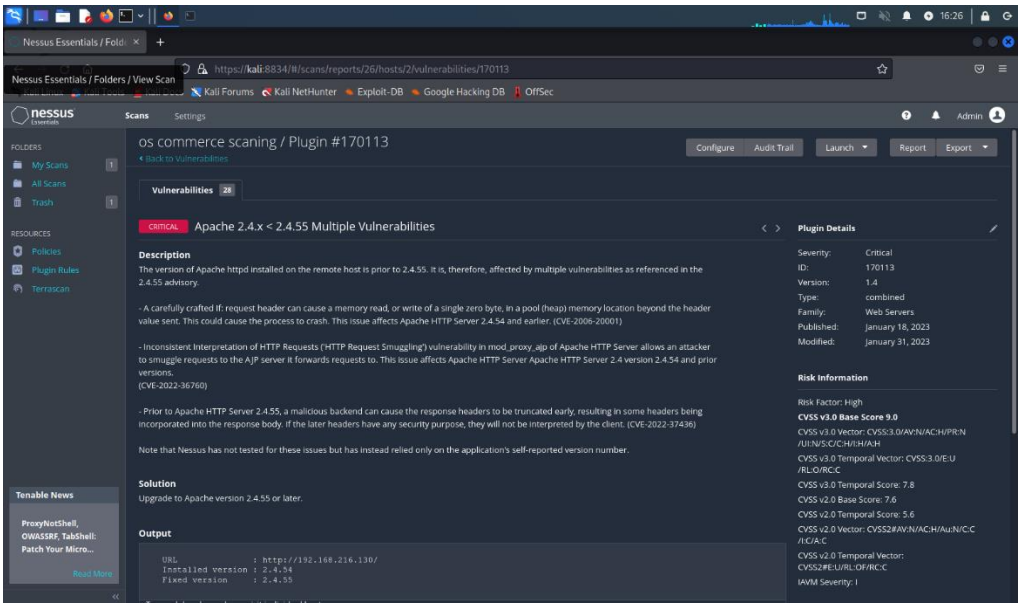
- Vulnerability: Accessible /install folder allowing reinstallation of the database, wiping all stored data, and potential administrative access.
- Vulnerability: Remote Control Execution no need authentication
- Vulnerability: Using http connection instead of https(unsecured network)

Other vulnerabilities detected after doing a Nessus Scan:

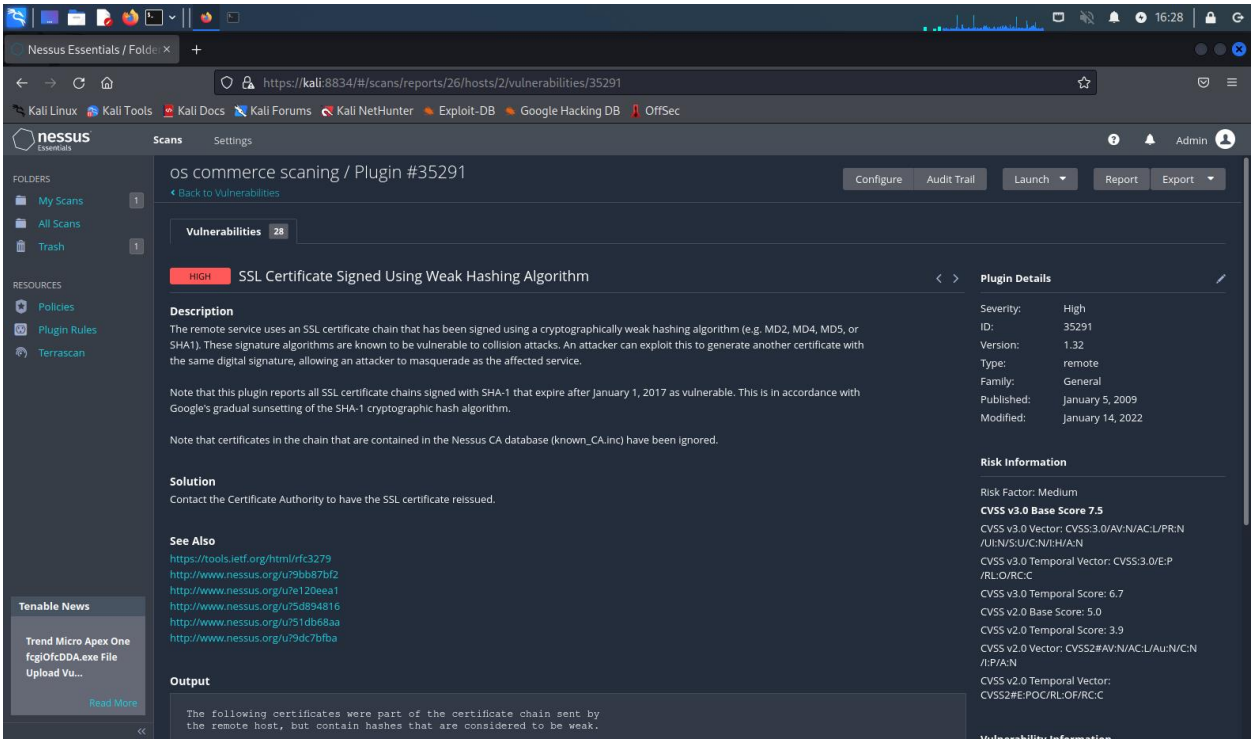
PHP Version vulnerability



Apache version vulnerability



Weak hashing algorithm vulnerability



6. EXPLOITATION AND REPORTS

6.1 Website hijacking

Vulnerability [1] : Website hijacking

Severity : Critical

Instance : http://target/oscommerce/catalog/install/

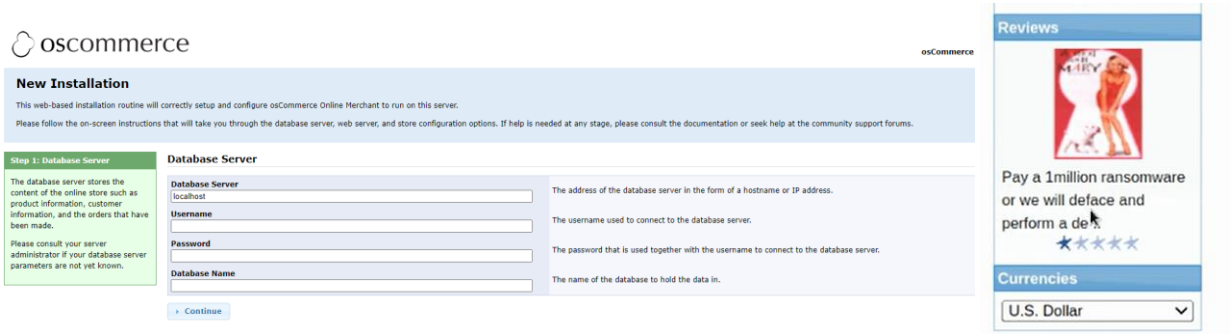
Description : One of the vulnerabilities found in OSCommerce version 2.3.4.1 is the ability for an attacker to hijack the website by finding the /install folder and reinstalling the database. This vulnerability is caused by the presence of the /install folder, which is used during the initial installation of the OSCommerce software. Once the software has been installed, the /install folder is typically removed, but in some cases, it is not, leaving the folder and its contents accessible to an attacker.

If an attacker can access the /install folder, they can use the scripts contained within it to reinstall the database, effectively wiping out all the data that is currently stored in the database and replacing it with a new, blank database. This can be used to delete all the data on the website, including customer information, product information, and order data, effectively rendering the website inoperable.

In addition to wiping out data, an attacker could potentially use this vulnerability to gain access to the website's administrative functions, allowing them to add, delete, or modify products, customer information, and other data on the website. This could be used to steal sensitive data, deface the website, or disrupt the business operations of the website.

Poc :

As you can see here after the attacker access the /install folder, he can simply start a new installation and he will be able to use new credentials and hijack the database and setup his own admin access to the website



The team was able to access and create a new database and changed the review into " Pay a 1million ransomware or we will deface and perform a denial of service"

Mitigation :

This vulnerability can be mitigated by ensuring that the /install folder is removed after the initial installation of the OSCommerce software, and by protecting the folder with proper permissions and access controls. Additionally, it is important to keep the OSCommerce software up-to-date with the latest security patches, as updates may include fixes for known vulnerabilities.

6.1 Remote Command Execution

Vulnerability [2] : Remote Command Execution

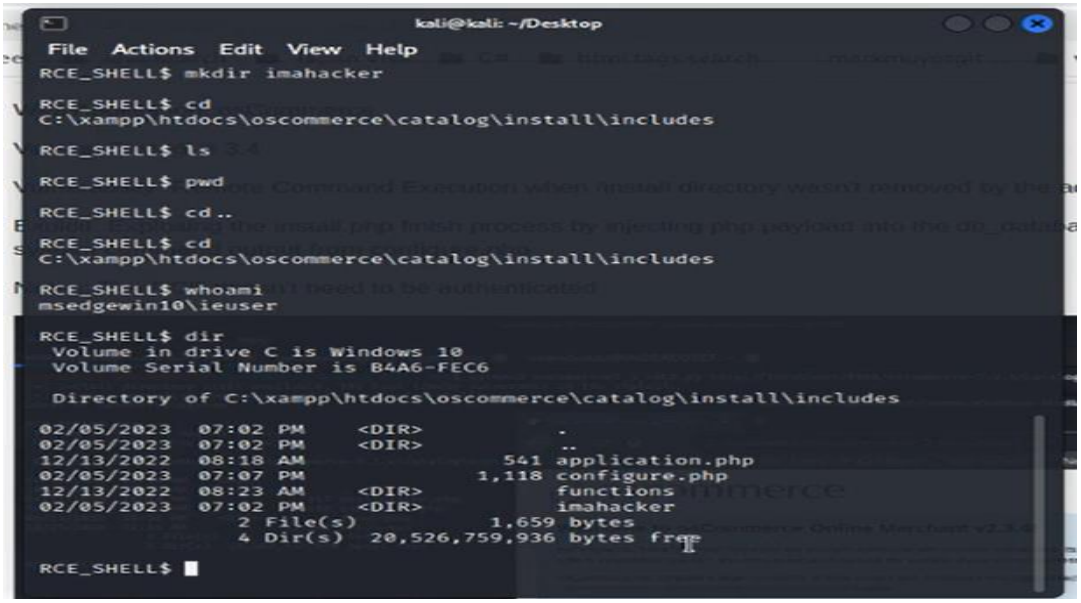
Severity : Critical

Instance : http://target/oscommerce/catalog/

Description : this vulnerability can allow an attacker to execute arbitrary code on the server by injecting malicious code into the "osCAdminID" parameter in the "login.php" script. The vulnerability is caused by a lack of proper input validation in the "login.php" script, which allows an attacker to inject malicious code into the "osCAdminID" parameter. This code is then executed by the server as part of the login process.

An attacker could use this vulnerability to gain unauthorized access to the server, steal sensitive information, or execute other malicious actions. They could also use it to upload and execute a webshell, allowing them to take control of the server.

Poc :



The team was able to run a python script: python3 osCommerce2_3_4RCE.py

http://192.168.100.5/oscommerce/catalog

This enable the team to perform a remote code execution from kali to web host which is windows 10 and performed this codes:

Whoami

To show what os and the user

Mkdir imahacker

This created a folder named imahacker

Mitigation :

This vulnerability can be mitigated by upgrading to the latest version of OSCommerce that has fixed this issue. Additionally, it is important to ensure that your software is always up-to-date and that you monitor your website for any suspicious activity. **Access rights:** Grant minimal access rights to individuals and team members — such as read only, read and write. Avoid allowing members, except the administrator leader, to have full access rights.

Run network intrusion detection system IDSs to monitor network traffic for malicious activity that may occur after an attacker exploits the Visual Studio Code vulnerabilities. Ensure IDSs are free of vulnerabilities as well.

7. RECOMMENDATION

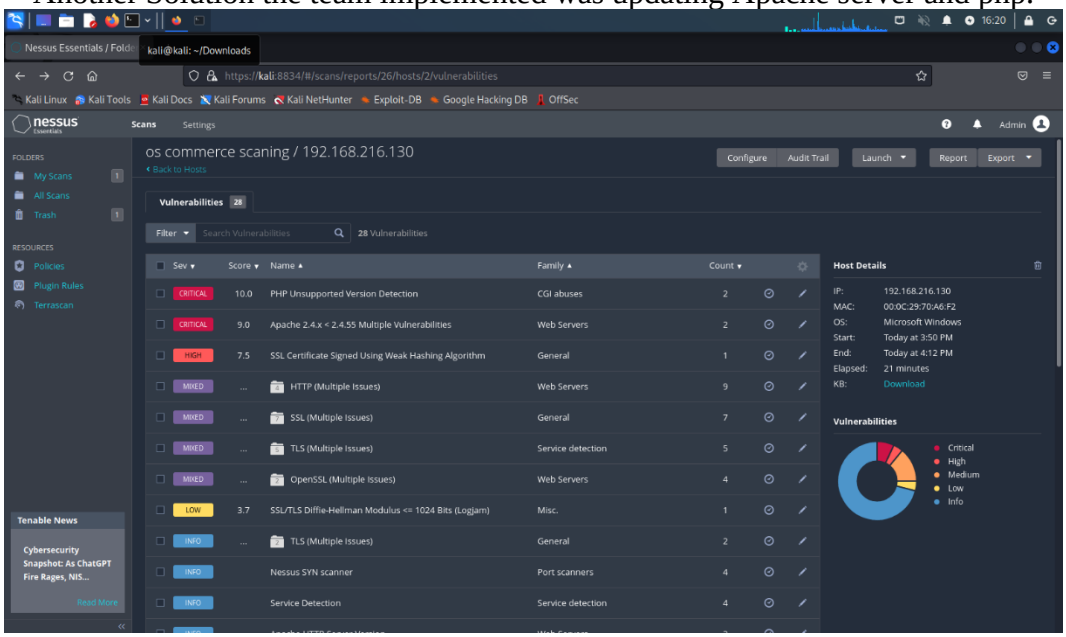
In conclusion, this paper analyzed the vulnerability assessment of osCommerce version 2.3.4.1, a widely used e-commerce platform. The assessment revealed two critical vulnerabilities that pose a significant threat to the security and privacy of the platform. The first vulnerability relates to the potential for cross-site scripting attacks, which can be used to inject malicious code into web pages viewed by other users. The second vulnerability is related to the lack of proper input validation, which can result in the injection of malicious SQL code and the theft of sensitive information from the database.

The assessment highlights the importance of keeping software up-to-date and implementing robust security measures such as limiting access rights to users, zero trust access, running a network intrusion detection system IDSs to protect against these types of attacks. Updating to a newer version of osCommerce can help to eliminate these vulnerabilities, and other security measures such as input validation and access controls can help to mitigate the risk of exploitation and enabling SSL/https.

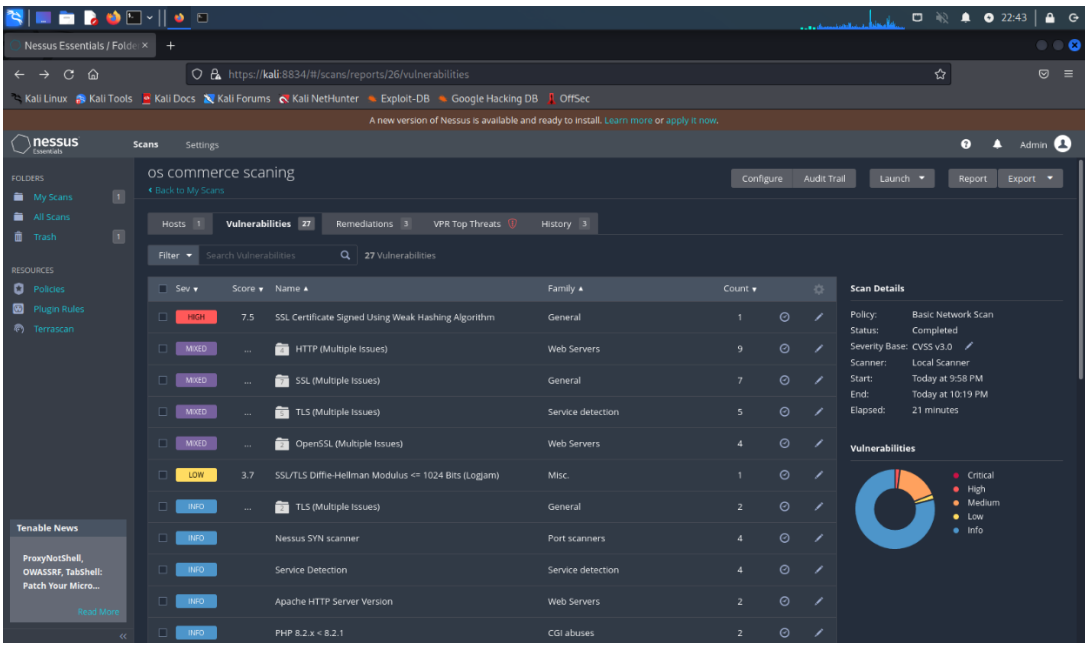
```
  AllowOverride All
  Require all granted
  </Directory>
</VirtualHost>

<VirtualHost 127.0.0.5:80>
  DocumentRoot "C:/xampp/htdocs/projects/sandbox/web"
  DirectoryIndex index.php

  <Directory "C:/xampp/htdocs/projects/sandbox/web">
  Options All
  AllowOverride All
  Require all granted
  </Directory>
</VirtualHost>

<VirtualHost 127.0.0.5:443>
  DocumentRoot "C:/xampp/htdocs/projects/sandbox/web"
  DirectoryIndex index.php
  SSLEngine on
  SSLCertificateFile "conf/ssl.crt/server.crt"
  SSLCertificateKeyFile "conf/ssl.key/server.key"
```

Sample on how to enable https on virtual host

Another Solution the team implemented was updating Apache server and php.



The first time we ran Nessus to scan for vulnerabilities we had this result



Nessus scan after updating Apache and php versions

8. CHALLENGES

In this project, our team encountered several challenges in conducting a penetration testing assessment. Despite having a foundation of knowledge from our class, we initially struggled with where to start and felt overwhelmed by the task at hand. However, we persevered and utilized the skills and techniques learned in class to the best of our ability.

One of the major challenges we faced was the time constraint, as we had other projects that demanded our attention. This made it difficult to allocate sufficient time and resources to our pen testing efforts, and we had to balance our priorities accordingly. The team also had a hard time figuring out how to set up an https connection.

Despite these challenges, we found this project to be an enriching and enjoyable experience. We learned a great deal about pen testing and web application security, and it was fulfilling to feel like professional hackers, even if it was only for a moment.

Overall, this project was a valuable learning experience for our team, and we will cherish the memories of staying up late and tackling the challenges of pen testing together.

9. REFERENCES

EC-Council. (n.d.). How to Write a Vulnerability Assessment Report. Retrieved from https://eccouncil.org/cybersecurity-exchange/ethical-hacking/how-to-write-vulnerability-assessment-report/

OWASP Foundation. (n.d.). OWASP Top 10. Retrieved from https://owasp.org/www-project-top-ten/#:~:text=The%20OWASP%20Top%2010%20is,step%20towards%20more%20secure%20coding.

GeeksforGeeks. (n.d.). How to Find Hidden Web Directories with Dirsearch. Retrieved from https://www.geeksforgeeks.org/how-to-find-hidden-web-directories-with-dirsearch/

CVEDetails.(n.d.).Oscommerce Oscommerce 2.3.4.1. Retrieved from https://www.cvedetails.com/vulnerability-list/vendor_id-1437/product_id-2485/version_id-599128/Oscommerce-Oscommerce-2.3.4.1.html

Ankit Chauchan. (2020, May). What is a Vulnerability Assessment? [Video file]. https://www.youtube.com/watch?v=0JScsUQGW7c

Exploit Database. osCommerce 2.3.4.1 - Remote Code Execution https://www.exploit-db.com/exploits/44374

Enabling https. Youtube https://ourcodeworld.com/articles/read/198/enabling-ssl-https-protocol-with-xampp-in-a-local-php-project