Executive Summary

A vulnerability scan was performed on the domain name of buymenow.org.uk, which uses AbanteCart, a free, open-source eCommerce software, which works with MySQL database. [J-P Briones, 2021]
The site has no failover server. The address (68.66.247.187) was registered to eNom LLC on 25-Apr-2022.

The report uses two tools: Nessus and Network scan.

Nessus determined a total of 46 alerts.

Critical	High	Medium	Low	Info
0	2	5	0	40

HIGH

- The host supports SSL ciphers, which are instructions that help establish a secure connection. This high threat was found on port 21, which uses the File Transfer protocol (FTP) and port 993, which is used for Internet Messaging Access Protocol (IMAP).

HIGH

- The host supports SSL ciphers, which are instructions that help establish a secure connection. Found on port 21, and port 993.

MEDIUM

- SSL Certificate is a way to establish a secure connection. The certificate has an incorrect hostname that is found for port 21 and port 993.
- The host supports anonymous SSL ciphers. This implies that an anonymous username can be used so no audit on what action or by whom this action was performed on port 21 and port 993.
- The host supports using the RC4, a type of cipher that operates on data, a byte at a time to encrypt. Several vulnerabilities were found, which meant that this could be cracked in less than a minute and RC4 is no longer a cipher that is recommended. [encryptionconsulting.com, no date]
- TLS Transport Layer Security, designed for data to be communicated over the internet securely, uses version 1.0, which is a deprecated version on ports 993 and 21.

The network identified open ports. An open port is a way for applications or protocols to allow for two-way communication with each other. Having secure ports open is not necessarily an issue, but having unsecured ports open with a default password set is a high alert.

From the results, ten ports are open. Out of these ten, only four were encrypted. Exposing six unencrypted ports. Four of these have no default password or

username. The two that do use passwords have the default password changed, reducing the threat and exposing this as a LOW alert.

As part of this report, an ad-hoc manual search of the internet was performed to see if any additional information could be found. The admin page still has the default setting, allowing the public to access the page [J-P Briones, 2021]
Although the page is available, the default password has been changed, reducing the exposure.

Having the admin page exposed provided version number 1.3.2. A number of threats existed before this version. The current version is bug-free and exposes this threat as an information alert. [cvedetails.com, no date]

2. Scan Results

Nessus Results

Threat	Description	Evidence	Recommendation	Alert Severity
SSL Medium Strength Cipher Suites Supported (SWEET32)	SSL ciphers that offer medium strength encryption	tcp/21/ftp Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)	Reconfigure the application and use high strength ciphers.	HIGH

SSL Medium Strength Cipher Suites Supported (SWEET32)	SSL ciphers that offer medium strength encryption	tcp/993/imap 68.66.247.187 6 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)	Reconfigure the application and use high strength ciphers.	HIGH
SSL Anonymous Cipher Suites Supported	use of anonymous SSL ciphers	tcp/21/ftp The following is a list of SSL anonymous ciphers supported by the remote TCP server Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)	Reconfigure the application and use high strength ciphers.	MEDIUM
SSL Certificate with Wrong Hostname	Incorrect Hostname specified	tcp/21/ftp The Common Name in the certificate is : *.a2hosting.com	Generate and update a certificate with the correct hostname	MEDIUM

		The Subject Alternate Names in the certificate are *.a2hosting.com a2hosting.com		
SSL Certificate with Wrong Hostname	Incorrect Hostname specified	tcp//993/imap The Common Name in the certificate is *.a2hosting.com The Subject Alternate Names in the certificate are 68.66.247.187 12 *.a2hosting.com a2hosting.com	Generate and update a certificate with the correct hostname	MEDIUM
SSL RC4 Cipher Suites Supported (Bar Mitzvah)		tcp/21/ftp List of RC4 cipher suites supported by the remote server High Strength Ciphers	Avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser	MEDIUM

			and web server support.	
Encrypts traffic using an older version of TLS.	TLSv1 is enabled and the server supports at least one cipher.		Enable support for TLS 1.2 and/or 1.3 and disable support for TLS 1.1.	MEDIUM

Network Result

PORT	Application Protocol	Type of Security	Default Password	Access Granted default value	Alert Severity
995	ssl/pop3	Encrypted	No default password	N/A	Info
110	pop3	Unencrypted	No default password	N/A	Info
143	imap	Unencrypted	No default password	N/A	Info

993	ssl/imap	Encrypted	No default password	N/A	Info
587	smtp	Encrypted	No default password	N/A	Info
25	smtp	Unencrypted	No default password	N/A	Info
80	http	Unencrypted	No default password	N/A	Info
443	ssl/http	Encrypted	No default password	N/A	Info
3306	mysql	Unencrypted	mysql : mysql mysql : root root : root	No	Low
21	ftp	Unencrypted	anonymous: anonymous	No	Low
53	domain	Unencrypted	No default password	N/A	Info

Manual Results

CVE code	Type of attack	Comments	Alert Severity

CVE-2021-42051	XSS	XSS Payload	info
CVE-2021-42050	XSS	DOM Based attack	info
CVE-2018-20141	XSS	Cross-site scripting attack	info
CVE-2022-26521	Exec Code	Remote authenticated administrators to execute arbitrary code	info

[CVEdetails.com, no date]

3. Evaluation of security standards

The first security standard, General Data Protection Regulation (GDPR), is a set of seven principles [ico.org.uk]. Some of these include personal and sensitive information about an individual such as name, location, an online username or the cookies the user has accepted. [Burgess. M, 2020]

A website review showed that no information was7 provided within the privacy policy on the website. When creating a new user, a tick box is present to ensure the user has read and agreed to the privacy policy. However, no details or information regarding what the policy entailed were provided, which is concerning. The alert is set to High.

The second security standard is the Payment Card Industry Data Security Standard (PCI DSS). Any business must be compliant if dealing with card holders' data, from

processing to storing. This needs to be done securely following the 12 principles. [RSI Security, 2018]

A review of the website indicated that the site accepted cards by showing an icon of a credit card. However, when trying to make a purchase, it stated that payment was required on delivery. Again, it is unclear if cash is needed or if a credit card is needed. This is raised to High alert.

4. Conclusion

In conclusion, the baseline report covered many details found in this report, which you can see below. The OWASP framework was an appropriate framework to use, and tools such as Netstat and Nessus complimented the framework to find the details outlined in this report. One thing to note is that the scan took a while to run, and at times the IP address running the scan would become blocked from the site as too much activity passed back and forth. To overcome this a custom scan was created tasking only specific items.

Threat	Definition	Justification
Malware Attack	Malicious software executed	Ports are open and possible attacks are present.

Traffic Analysis attack	Monitor network traffic Unused open ports	Open Ports found

Injection	Sending harmful packets within the network Executing harmful OS commands to the Operating System Executing SQL command to the database Manipulating JavaScript vulnerability	The below CVE was found but for older versions. CVE-2016-10755 CVE-2018-20141 CVE-2021-42051 CVE-2021-42050 [Teo and Chong, 2022]
Data protection standards	Follow the UK Data Protection standards	No Information

5. Recommendations

- Create a privacy and data policy following the GDPR.
- Adopt a PCI DSS standard or make it clear that no card payments are accepted.
- Generate and update a certificate with the correct hostname for FTP and IMAP applications.
- Reconfigure the applications to use TLS 1.2 or 1.3 and disable support for TLS 1.1 and RC4.
- Review the following open ports.

    3305 - MYSQL

    21 - FTP

    53 - Domain

References

Briones, J-P (2021) How to Access AbanteCart Admin Panel. Available from : https://www.inmotionhosting.com/support/edu/software/abantecart/how-to-access-abantecart-admin-panel/[Accessed 20 July 2022]

Briones, J-P (2021) What is AbanteCart? Available from : https://www.inmotionhosting.com/support/edu/software/abantecart/what-is-abantecart/[Accessed 20 July 2022]

BURGESS, M (2020) What is GDPR? The summary guide to GDPR compliance in the UK Available from : https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018#:~:text=GDPR's%20seven%20principles%20are%3A%20lawfulness,new%20to%20data%20protection%20rules.
[Accessed 20 July 2022]

CVEdetails.com The ultimate security vulnerability data source Available from: https://www.cvedetails.com/version/676819/Abantecart-Abantecart--.html [Accessed 20 July 2022]

encryptionconsulting.com What is RC4? Is RC4 secure? Available from: https://www.encryptionconsulting.com/education-center/what-is-rc4/[Accessed 20 July 2022]

ico.org.uk/ The principles Available from:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/
[Accessed 20 July 2022]

rsisecurity.com TYPES OF DATA SECURITY STANDARDS Available from:
https://blog.rsisecurity.com/types-of-data-security-standards/
[Accessed 20 July 2022]

Teo D and Chong I(2021) Multiple vulnerabilities in AbanteCart e-commerce platform Available from:
https://sec-consult.com/vulnerability-lab/advisory/multiple-vulnerabilities-in-abantecart-e-commerce-platform/
[Accessed 20 July 2022]