Unit 4: Scanning and Collaborative Wiki Activity

The answers provided below are related to the website pamperedpets.org.uk. I used the Linux Kali tools to gather the necessary information for this activity. My objective was to explore vulnerabilities in the website and identify any potential areas for improvement. The information obtained using Linux Kali will further analyse the website's content and structure and will be added to my final assessment report.

1. **What Operating System does the website utilise?**
   - The operation system used is Apache, according to the Whatweb tool.

2. **What web server software is it running?**
   - The website's web server is HTTPServer, according to the Nikto tool.

3. **Is it running a CMS (WordPress, Drupal, etc.?)**
   - The Website is running Joomla according to the SMSeek tool.

4. **What protection does it have (CDN, Proxy, Firewall?)**
   - The site pamperedpets.org.uk seems to be behind a WAF or security solution, according to the wafw00f tool.

5. **Where is it hosted?**
   - Is hosted in a2webhosting.com.

6. **Does it have any open ports? Which did you expect to be open?**
   - The following ports were identified running the Nmap tool:

PORT	STATE	SERVICE
21/tcp	open	ftp
80/tcp	open	http
110/tcp	open	pop3
143/tcp	open	imap
443/tcp	open	https
993/tcp	open	imaps
995/tcp	open	pop3s
3306/tcp	open	mysql
5432/tcp	open	postgresql

7. **Does the site have any known vulnerabilities?**
   - The following are the vulnerabilities I have identified running the Testssl tool:

Vulnerability	Severity	Status	Comments
Heartbleed (CVE-2014-0160)	Critical	Not Vulnerable	No heartbeat extension
CCS (CVE-2014-0224)	Critical	Not Vulnerable	
DROWN (CVE-2016-0800, CVE-2016-0703)	Critical	Not Vulnerable	Check SSLv2 usage on other services.
Ticketbleed (CVE-2016-9244)	High	Not Vulnerable	Experiment. No vulnerability was detected.
ROBOT	High	Not Vulnerable	The server does not support any cipher suites that use RSA key transport
LUCKY13 (CVE-2013-0169)	High	Potentially Vulnerable	Uses CBC ciphers with TLS. Check for patches.
Winshock (CVE-2014-6321)	High	Not Vulnerable	
BREACH (CVE-2013-3587)	Medium	Potentially Not OK	"gzip" HTTP compression detected. It can be ignored for static pages or if there are no secrets on the page.
POODLE, SSL (CVE-2014-3566)	Medium	Not Vulnerable	No SSLv3 support
LOGJAM (CVE-2015-4000)	Medium	Not Vulnerable	No DH EXPORT ciphers, no DH key detected with <= TLS 1.2
BEAST (CVE-2011-3389)	Medium	Not Vulnerable	No SSL3 or TLS1 support
Secure Renegotiation (RFC 5746)	Low	Supported	
Secure Client-Initiated Renegotiation	Low	Not Vulnerable	
CRIME, TLS (CVE-2012-4929)	Low	Not Vulnerable	
TLS_FALLBACK_SCSV (RFC 7507)	Low	No Fallback	No fallback was possible. No protocol below TLS 1.2 Offered
SWEET32 (CVE-2016-2183, CVE-2016-6329)	Low	Not Vulnerable	
FREAK (CVE-2015-0204)	Low	Not Vulnerable	
RC4 (CVE-2013-2566, CVE-2015-2808)	Low	Not Vulnerable	No RC4 ciphers detected

8. **What versions of software is it using? Are these patched so that they are up to date?**

- Apache PHP - 7.4.33, according to Testssl tool. No, it has not been updated since the latest version is 8.2.0. According to Tenable (2022), PHP 7.4.x < 7.4.33 has multiple vulnerabilities.

Reflection

During the activity, I faced several challenges that required my full attention to overcome. The most significant challenge was setting up a Kali Linux virtual machine on my PC, which took me two days to accomplish. The process involved installing the proper repositories and testing my website, which presented several difficulties. However, my previous experience with CentOS came in handy as there were some similarities between the two systems. I conducted extensive research and used my knowledge to troubleshoot and solve the problem. Eventually, I could make it work, but the experience taught me the importance of persistence and problem-solving skills in overcoming complex challenges.

I must admit that investing in Kali Linux has proven to be an invaluable decision. Its integration into my website scanning process has yielded much more comprehensive and detailed results, providing me with a wealth of information about my final assessment. The insights I have gained through this investment have been crucial in helping me improve the quality of my work and make better-informed decisions.

During this activity, I gained a valuable understanding of hackers' vulnerabilities and exploits to control websites and exploit weaknesses. I was able to delve deeper into the thought process of a hacker and understand the techniques they use to exploit vulnerabilities. This experience has given me a comprehensive understanding of how websites can be compromised and the importance of implementing robust security measures to prevent such attacks. This activity has significantly enhanced my knowledge and awareness of cybersecurity and its importance in today's digital world.

References:

- Tenable (2022). *PHP 7.4.x < 7.4.33 Multiple Vulnerabilities*. [online] Available at: https://www.tenable.com/plugins/nessus/166901 [Accessed 3 Dec. 2023].