The blog site allmytype.co.uk is a public-facing website based in the UK. As a result, it is potentially vulnerable to numerous cyber threats. It was previously hypothesized that the website was vulnerable to several different types of cyberattacks. Attacks such as malware, infrastructure exploitation, DDoS attacks, On path attacks, and Data leakage. To test these hypothesized vulnerabilities, several web-based vulnerabilities scans were run as referenced in figure 1.

The first scan that was run was OWASP Zap. The OWASP Zap tool was made by the Open Web Application Security Project (OWASP), one of the most popular sites for providing free web applications security information (zaproxy, 2022). The tool itself is open source, which provides extra credibility, due to the exposure of code, nothing malicious or unwanted could be hidden within it. With the tool, an automated scan was run that returned nine vulnerabilities.

The second scanner used was Burp Suite. Burp Suite is an enterprise-level vulnerability scanner. It is one of the most highly rated scanners on the market. With the tool, a web crawl and passive audit were conducted on the target website. The tool was made with web scanning in mind, and as such is great for detecting common web vulnerabilities such as cross-site scripting(XSS) (portswigger, 2022). During the performed scan five vulnerabilities were found, with one being XSS.

The third scanner used was skipfish. Skipfish is a tool built into Kali Linux. It performs “recursive crawl and dictionary-based probes” (Kali, 2022). It is a simple but efficient tool that provides quick scans. Within the scan conducted by it, three main vulnerability types were discovered.

The fourth scanner ran was Nikto. A tool that is built into Metasploit, which is one of the most highly regarded penetration toolsets (Bhatt, 2018). Nikto is an open-source web server and application scanner that provides very fast scans(Shivanandhan, 2021). It also is relatively simple to use but allows for a diverse amount of scans to be run. Within its scan, it discovers five different vulnerabilities.

The final scanner used was Nmap. Nmap is the most commonly used port scanning tool. It works by “querying raw IP packets to determine available hosts and network services'' (Bhingardeve & Franklin, 2018). For the given situation it was used to query the blog site in mention. The results were 21 ports that were open that could potentially be exploited.

| **Name** | **Test Carried Out** | **Vulnerabilites Discovered** |
| --- | --- | --- |
| OWASP ZAP | Automated Web Scan | Vulnerable JS Library |
|  |  | Absence of Anti\_CSRF Tokens |
|  |  | Cookie No HttpOnly Flag |
|  |  | Cookie without SameSite Attribute |
|  |  | Incomplete or No Cache-Control Header Set |
|  |  | Server Leaks |
|  |  | Information Disclosure - Suspicious Comments |
|  |  | Timestamp Disclosure - Unix |
| Burp Suite | Audit and Passive Crawl | DOM Based XSS |
|  |  | Cookie without HttpOnly flag set |
|  |  | Vulnerable JavaScript Dependency |
|  |  | Password Field with autocomplete enabled |
|  |  | Unencrypted communications |
| SkipFish | Automated Web Scan | External Content embeeded on a page. 112 high risk instances. |
|  |  | External Content embeeded on a page. 3 low risk instances. |
|  |  | SSL certificate host name mismatch |
| Nikto | Automated Web Scan on HTTP and HTTPS | Anti-Clickjacing X-Frame option header Is not present |
|  |  | X-XSS hearder is not defined |
|  |  | X-Content type options header is not set |
|  |  | Strict transport security HTTP header is not defined |
|  |  | Expect-CT header is not present |
| Nmap | Port Scan | Open TCP Port 53,21,80,110,143,554,993,2078,2079,2080,2082,2083,2087,2096,2095,2525,3306,5432,6556,7822,46414 |

Figure 1. Vulnerability Scans.

References:

Bhatt, D. (2018) Modern Day Penetration Testing Distribution Open Source Platform - Kali Linux - Study Paper. *International Journal Of Scientific & Technology Research.* 7(4): 1-5. Avaliable from:<https://www.ijstr.org/final-print/apr2018/Modern-Day-Penetration-Testing-Distribution-Open-Source-Platform-Kali-Linux-Study-Paper.pdf>

Bhingardeve, N. & Franklin, S. (2022) A Comparison Study of Open Source Penetration Testing Tools. *International Journal of Trend in Scientific Research and Development. 2*(4): 1-3. DOI:<https://doi.org/10.31142/ijtsrd15662>

Kali. (2022) Skipfish Usage Example. Available from:

<https://www.kali.org/tools/skipfish/> [Accessed 23 Janurary 2022].

PortSwigger. (2022) Using Burp to Find Cross-Site Scripting Issues. Avaliable from:<https://portswigger.net/support/using-burp-to-find-cross-site-scripting-issues> [Accessed 22 Januray 2022].

Shivanandhan, M. (2021) Web Serrver Scanning With Nikto – A Beginner’s Guide. Avaliable from:<https://www.freecodecamp.org/news/an-introduction-to-web-server-scanning-with-nikto/> [Accessed 22 January 2022].

Zaproxy (2022) Getting Started. Available from:<https://www.zaproxy.org/getting-started/> [Accessed 30 January 2022].