**What Operating System does the web site utilise?**

Firstly, I used command ns lookup tool to find out the IP address of the specific domain shown below. nslookup is a simple tool which is used to find the IP against the domain.

Shape

Description automatically generated with medium confidence

Figure 1. NSLOOKUP tool result

Then I applied different tools like nmap and whatweb to find out the OS of the web The screenshot of both the tool is given below. The OS of this web server is Windows. The results that I got from the tools are given below.

Text

Description automatically generated

Figure 2. Nmap Result

Text

Description automatically generated

Figure 3. WhatWeb Results

**What web server software is it running?**

The Server they are using is Apache, the scanning report is shown in below figure. We can find it from different tools but the tool that I used is dnsdumpster and whatweb.

Text

Description automatically generated

Figure 4. Server Details

**Is it running a CMS (WordPress, Drupal, etc.?)**

Yes, they are running the WordPress version 5.8.2, I was able to find it through the tools dnsdumpster and the result of the screen shot is given below.

Shape

Description automatically generated with medium confidence

Figure 5. WordPress Version

**What protection does it have (CDN, Proxy, Firewall?)**

Yes, they are using the firewall of Cloudflare the below screen shot it shown that how we find it. We found it through the dnsdumpster tool.

**Graphical user interface

Description automatically generated**

Figure 6. Cloud Flare Firewall

Graphical user interface, application

Description automatically generated

Figure 7. Cloudflare net

**Where is it hosted?**

It is hosted in United State and hosted by A2HOSTING.

Text

Description automatically generated

Figure 8. Hosted Location and hosted by.

**Does it have any open ports?**

Yes, there are 4 open ports in it which is shown in the below figure.

Graphical user interface, text

Description automatically generated

Figure 9. Nmap Scan for open ports

**Does the site have any known vulnerabilities?**

I tried this domain on different online and kali linux scanner to found out the vulnerabilities in it. But all the tools that I used was not giving me a satisfying result then I tried a tool name HostedScan, and I found their result was good and all the result is shown given below. I found out the 27 risks which was medium and low. These results are based on tools which are Nmap and OWASP\_ZAP. Nmap and OWASP\_ZAP are also kali linux tools.

Graphical user interface, table

Description automatically generated with medium confidence

Figure 10. ZAP and NMAP results

Table

Description automatically generated with low confidence

Figure 11. NMAP Results

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

They are using word press 5.8.2 and this is not a latest version basically latest version is 5.9 and the version they are using is patched.