**Scanning and Collaborative Wiki Activity**

* **What Operating System does the website utilise?**
  + The selected website (ehr-online.co.uk/) uses Linux as its OS.
* **What web server software is it running?**
  + The selected website (ehr-online.co.uk/) uses Apache as its web server.
* **Is it running a CMS (WordPress, Drupal, etc?)**
  + No, it is not running any CMS.
* **What protection does it have (CDN, Proxy, Firewall?)**
  + It does not have a firewall, but it has H2 Application-Level Protocol Negotiation (ALPN), which is a Transport Layer Security (TLS) extension that enables the application layer to negotiate which protocol should be performed via a secure connection.
* **Where is it hosted?**
  + It is hosted in Amsterdam, the Netherlands.
* **Does it have any open ports? Which did you expect to be open?**
  + Yes, it has 13 open ports. Nevertheless, the following 4 ports are expected to be open: port 53 for DNS; port 443 for HTTPS (encrypted) traffic; port 993 as a secure port for IMAP, which works via TLS/SSL encryption; port 995 as the encrypted port for POP3, which also works over TLS/SSL.
* **Does the site have any known vulnerabilities? What versions of software is it using? Are these patched so that they are up to date?**
  + Six publicly known vulnerabilities were identified due to running an outdated version (1.4.3) of jQuery, including cross-site scripting and prototype pollution, as ranked in descending order of their CVSSv3.1 score in the table below. This component should be urgently updated to the latest version 3.6.0.
  + The 9 ports that should not be open may be dangerous when the service listening on such ports is not configured properly, without the required patches, vulnerable to exploits, or has poor network security.

| **CVSSv3.1 score** | **Vulnerability CVE-ID** | **Vulnerability Type** |
| --- | --- | --- |
| 5.5 Medium | CVE-2020-7656 | CWE-79 — Cross-site scripting |
| 5.5 Medium | CVE-2020-11022 | CWE-79 — Cross-site scripting |
| 5.3 Medium | CVE-2015-9251 | CWE-79 — Cross-site scripting |
| 5.3 Medium | Not Assigned | CWE-79 — Cross-site scripting |
| 4.8 Medium | CVE-2019-11358 | CWE-400 — Prototype pollution |
| 4.1 Medium | CVE-2020-11023 | CWE-79 — Cross-site scripting |

* **Did you have any issues or challenges with the scans?**
  + No, I did not.
* **How did you overcome them?**
  + Besides leveraging the tools on Kali Linux, I leveraged online scanners too, which are tailored to specific tasks, such as CMS detection for instance.
* **How will they affect your final report?**
  + I will continue to leverage multiple tools for deriving more comprehensive findings and recommendations in the final report.