Scanning Exercise and Collaborative Learning Wiki

* What Operating System does the web site utilise?
  + Linux 2.6.32
* What web server software is it running?
  + Apache
* Is it running a CMS (Wordpress, Drupal, etc?)
  + No
* What protection does it have (CDN, Proxy, Firewall?)
  + Unknown
  + Lacks SSL/TLS
* Where is it hosted?
  + Ec2-35-175-70-228.compute-1.amazonaws.com
  + AWS EC2
* Does it have any open ports?
  + 22
  + 80
  + 443
* Does the site have any known vulnerabilities?
  + The remote SSH server is configured to allow weak encryption algorithms (datatracker.ietf.org).
  + MacOS X creates a hidden le '.DS\_Store', in each directory that has been viewed with the 'Finder'. This file contains a list of the contents of the directory, giving an attacker information on the structure and contents of your website (www.securityspace.com, 2021).
  + X-Frame-Options Header Not Set (zaproxy.org, 2021).
* What versions of software is it using? Are these patched so that they are up to date?
  + OpenSSH 7.4

# References

datatracker.ietf.org *Encryption*. Available at:<https://datatracker.ietf.org/doc/html/rfc4253#section-6.3>.

www.securityspace.com (2021) *MacOS X Finder '.DS\_Store' Information Disclosure*. Available at:<https://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.10756>

zaproxy.org (2021) *X-Frame-Options Header Not Set*. Available at:<https://www.zaproxy.org/docs/alerts/10020-1/>.