Remediation of vulnerable and weak cipher suites in **Apache** and **NGINX** Servers.

 ----Be aware that limiting the cipher suites on a web server could potentially cause older browsers to be unable to connect with the resource in question due to the outdated browser not supporting it.

There are multiple ways to remediate weak and vulnerable cipher suites. The most common methods along with the most common web servers: Apache and Nginx. There are small differences between these two configurations, choices are based on the web server you use.

It is important to note that support for cipher suites is determined by your OpenSSL installation and not the web server itself. OpenSSL should be up to date before proceeding with these instructions.

Apache Web Servers

Configuration file name: httpd.conf OR .htaccess if configuring for a specific directory

More information about hardening the SSL configuration of Apache can be found here: https://httpd.apache.org/docs/trunk/ssl/ssl_howto.html

Open the configuration file and add these lines:

```
# This Line will disable SSLv3, TLSv1 and TLSv1.1
# If you have some browsers unable to connect without TLSv1.1, you can enable that again. Simply remove it from this line.
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1

# Enable modern TLS cipher suites, separated by colons
# These cipher suites may not all be supported by TLSv1.1 if it's enabled
# Please ensure that you are using a modern version of OpenSSL before proceeding with these suites!!
SSLCipherSuite  ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256

# The order of cipher suites matters, so this next line will force the ordering
SSLHonorCipherOrder on

# Disable TLS compression, preventing TLS compression oracle attacks (AKA the CRIME attack)
SSLCompression off

# Necessary for the security of Perfect Forward Secrecy, especially if the server isn't restarted very often
SSLSessionTickets off
```

NGINX Web Servers

Configuration File Name: ssl.conf

More information on NGINX hardening can be found here:
https://geekflare.com/nginx-webserver-security-hardening-guide/

You want to open your ssl.conf and add these lines:

```
# This line will only allow the TLSv1.2 protocol.
ssl_protocols TLSv1.2;

# Uncomment the next line if you require TLSv1.1 support, and comment the line above
# ssl_protocols TLSv1.1 TLSv1.2;

# Enable Modern TLS Cipher Suites, separated by colons
# These cipher suites may not all be supported by TLSv1.1
ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384
EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH
EDH+aRSA HIGH !RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS";
```