Generate DH parameters (dhparam.pem)

One of the things we can do to improve the security of our website is to generate our own DH parameters. What these parameters mean is decently explained HERE.

Genreate dhparam.pem

```
$ openssl dhparam -out dhparam.pem 4096
```

If you are generating directly into the `/etc/nginx` directory (only writable by root), you can use `sudo`, or if you don't want to elevate `openssl` for no reason, just generate the file to a writable location and copy it to `/etc/nginx` later on.

```
$ sudo openssl dhparam -out dhparam.pem 4096
```

> Heads up – This will take a long time, especially on less powerful servers/VMs.

Add it to Nginx config

Open Nginx configuration file and add the path to `dhparam.pem` file under the `server` block.

```
$ sudo vi /etc/nginx/conf.d/your_config_file.conf
```

```
...
ssl_dhparam /etc/nginx/dhparam.pem;
...
```

Test the configuration to avoid mistakes (like forgetting `;`) etc.

```
$ sudo nginx -t
```

Restart Nginx to apply the change:

```
$ sudo systemctl restart nginx
```

Revision #3
Created 30 September 2021 00:40:17 by Marek
Updated 30 September 2021 00:50:43 by Marek