**STRATEGIES TO SECURE OUR SYSTEM**

1. **Password Encryption and salting**

Passwords should not be stored in plain text format or md5 format. We have already implemented this.

1. **Installation of SSL**

We have installed a security certificate to help identify our website as the genuine one.

1. **Backup**

In case of a data loss, we should be able to able to recover our system files and database. We have a comprehensive storage for system files. Our database backup is not real time but a snapshot at a particular point in time.

1. **Server configuration**

Our nginx.conf has passed the configuration test, all permissions set up

1. **Folder Permissions**

Folder permissions are well configured.

1. **DDOS Protection**

No counter-measures have been set up thus far

1. **Database injection protection.**

Protection is In-built into our laravel project

1. **Fire wall protection**

We don’t have any measures set up at the moment.

1. **Secure Account Recovery**

Needs checks.