Security Documentation

# HTTPS deployment

Only using https minimizes man-in-the-middle attacks as communications between the client and server are encrypted.

# Server-side sanitization

All user input is passed though htmlspecialchars(). This removes html tags and other special entities preventing XSS attacks.

# Prepared statements

Eliminate SQL injection.

# Directory security

## Hidden directories

All asset directories are hidden using a index.php file which shows a 404 page. This is an example of security through obscurity.

## Forbidden directories

Directories used only by the server are disabled from the user via htaccess.

# Password security

## Strong passwords

Users are required to use strong passwords.

## Hashed passwords

Passwords are stored using modern hashes with salts and never in plain text format eliminating the risk of user passwords being made public in the event of network intrusion.

# reCAPCHA

Prevent bots from registering accounts and autonomous use of website.