Authorization / Security

Authorization is the process of determining which permissions a person or system is supposed to have.

Ex:

An admin should be able to create blog posts and delete comments, a regular user should only be able to add comments

How?

Simple

- Add a `admin` boolean on every user

```
{
  username: "Rob",
  password: "rob",
  admin: true
}
```

Advanced

- permissions collection
- give users an array of permissions and look up in the permissions collection

```
{
  role: 'admin'
  edit_page: true,
  create_posts: true,
  delete_posts: true,
  edit_posts: true,
  add_comments: true,
  delete_comments: true
},
{
  role: 'user',
  edit_page: false,
  create_posts: false,
  delete_posts: false,
  edit_posts: false,
  add_comments: true,
  delete_comments: false
}
```

```
{
  username: 'rob',
  role: 'admin'
}
```

Password Security

- `bcrypt` is a key derivation function for passwords
- one way function
- uses a salt
- pass the password back in and see if it matches

PCI Compliance

- SSL connection
- PCI compliant data center with firewalls etc
- Compliance Audits etc.
- Credit Card numbers never stored as plain text