Data security

- Passwords should only be stored in encrypted format: so they can be compared with (encrypted) user input but never exposed
- Organisations which send your password to you on request must be storing the data in unencrypted form! Instead, give option to user to reset their password. http://plaintextoffenders.com !!!
- Https should be used systematically in all security-critical parts of a website.

  In 2016 there is no excuse not to use HTTPS

  See: https://letsencrypt.org

Remove web-specific coding from business tier

Business tier code should not refer to HTTP request structures:

```
public class House
{ String address;
  String style;

  public House(HttpServletRequest req)
  { address = req.getParameter("address");
    style = req.getParameter("style");
  }
}
```

Using *HttpServletRequest* as input parameter type prevents non-web clients from using this business object. Instead, use data based on PIM or PSM class diagram of the system:

```
public class House
{ String address;
  String style;

  public House(String addr, String stl)
  { address = addr;
    style = stl;
  }
}
```