v4 Compatibility

Generally, apps running in v3 are compatible in v4. However, there is greater emphasis on security in v4 so the following exceptions apply:

1. **Form Elements** - Form labels and values now do not allow script execution to prevent possible cross-site scripting (XSS) vulnerabilities. Apps that depend on scripting will need to place such scripts into Custom HTML elements.
2. **Readonly Form Elements** - Previously, form read-only field values are not editable in the browser, but get stored in the database upon form submission. In v4, read-only field values are no longer stored to prevent unintended modifications using client-side browser tools such as Browser Console, Firebug, etc.
3. **JSON API Request Methods** – Previously, JSON API calls that modify the state of a process (e.g. start a process, complete an assignment, etc) support both HTTP GET and POST. In v4, only POST requests are supported to prevent cross-site request forgery (CSRF) attacks. Read-only API calls are unchanged. Please refer to the latest JSON API reference in the Knowledge Base at JSON API
4. **JSON API Responses** – In v4, all JSON API calls respond with JSON responses only. Previously, failed authentication will redirect the request to a login page, but a failed authentication now would result in a JSON 401 response e.g.

   ```
   {"error":{"message":"","code":"401","date":"Fri Feb 28 17:41:59 MYT 2014"}}
   ```

5. **JSON API Authentication** – The JSON API now supports basic authentication, so this would be the recommended authentication mechanism when combined with HTTPS.
6. **JavaScript API Authentication** - Previously, in the JavaScript API AssignmentManager.login(url, username, password, callback), the password can be either the plaintext password or user hash. In v4, user hash is only accepted in a separate call AssignmentManager.loginWithHash(url, username, hash, callback)

Apps that make use of the above may need to be modified and tested accordingly.