Foodika web application setup guide

Setup security tips

Whenever you want to install a Foodika instance somewhere (not matter in dev mode or production, you should perform some checks to make sure you are safe enough to deploy the application.

Check1 – Required: change variables in **.env** and **.dev.env** files. The variables are:

1. SITE_NAME: Optional
2. SITE_TITLE: Optional
3. PORT: Optional
4. OTHER_PORT: Optional
5. TZ: Optional
6. MAXIMUM_IMAGE_SIZE: Optional
7. ALLOWED_FILE_EXTENSIONS: Optional
8. ALLOWED_MIME_TYPES: Optional
9. FOODS_IMAGE_LOCATION: Optional
10. FOODS_DEFAULT_IMAGE: Optional
11. DOMAIN: **Required**
12. CSRF_SESSION_KEY: **Required**
13. JWT_SECRET: **Required**
14. SESSION_SECRET: **Required**
15. DEFAULT_ADMIN_USERNAME: **Required**
16. DEFAULT_ADMIN_PASSWORD: **Required**
17. MONGODB_URI: **Required**
18. NEXTPAY_API_KEY: **Required**

Check2 – Required: If your server/host supports HTTPS (that is recommended to be), you should secure you cookie session. Look for a line with comment:

```
// secure: true for production when SSL available
```

And change the value to true.

Check3 – Required: Change AES key for the client side encryption and decryption inside main script called foodika.js. The key stored in a module named security.

Check4 – Required: All your keys should be cryptographically random and they should be 4096 bytes minimum. One of the best ways to generate keys is using the crypto module from node itself just like:

```
1.  var s = require("crypto");
2.  s.randomBytes(4096).toString("base64");
```

Check5 - Required: You should manage permissions for files db-start.sh and app-start.sh, otherwise that could be lead to file mis-configuration vulnerability and cause system PWN!

Check6 - Required: If you are not a developer or someone from dev team and you want to add features to the app, ONLY and ONLY be in touch with the dev team and DON'T change codebase yourself.

Check7 - Optional: If you want to experience more security and stability, obfuscate main script called foodika.js (don't obfuscate function or modules names).

Check8 - Optional: If you want to deploy Foodika on a container (like docker etc.), it's better to install docker on a VM system to completely separate app instance from the main server.

Check9 - Optional: It's better for you to use authorized account for mongoDB database on the application's database (called as Foodika).