Security Configurations

We are working on a special sprint enhancing security to prevent software vulnerabilities in all the OMK Applications.

Versions affected:

- opCharts 4.2.5
- opConfig 4.2.4
- opEvents 4.0.2
- opHA 3.3.1
- opReports 4.2.2

Randomize Secrets

New setup tool to randomize the secrets from the command line. This tool will randomize *omkd_secrets* tokens in OMK and also, NMIS *auth_web_key* when it matches some of the OMK tokens (Usually set to configure SSO).

This tool is also called by the installer and fixed CVE-2021-38551.

Usage instructions:

```
/usr/local/omk/bin/opcommon-cli.exe act=secrets_randomise [force=true] [length=N]
```

Where:

- force=true will change the token even if this is not the default (Like =~ change_me)
- length=N will force the token length to N (32 by default)

Cookies

Cookie	Support	Behaviour
HttpOnly	✅ By default	The cookies are not going to be accesible from the JavaScript API.
secure	✅ Should be enabled by setting the configuration item "*auth_secure_cookie*" => "true" in opCommon.json.	This cookie could be sent just in a request ciphered over **https** protocol. That's the reason why it is not set by default.
SameSite set to *Strict*	⚠️ Will be supported in next versions. (Major version upgrade from libraries is required)	The cookie set to strict means that the browser just send the cookie if the request was made in the website that originally stablished the cookie.

Security Content Policy

The Security Content Policy is a http header that restricts how resources (JavaScript, CSS, Images, etc.) are loaded from allowed sites. It will help to mitigate some attacks of Cross Site Scripting (XSS) and data injection.

The default values can be overwritten setting the configuration item **security_content_policy** in the configuration file, opCommon.json.