CSRF Protection

Cross-site request forgery (also known as CSRF or XSRF) is a type of malicious exploit of a website where **unauthorized** commands are transmitted from a user that the web application trusts. To mitigate this kind of attack you can use the csurf package.

Use with Express (default)

Start by installing the required package:

```
$ npm i --save csurf
```

> warning **Warning** This package is deprecated, refer to `csurf` docs for more information.

> warning **Warning** As explained in the `csurf` docs, this middleware requires either session middleware or `cookie-parser` to be initialized first. Please see that documentation for further instructions.

Once the installation is complete, apply the `csurf` middleware as global middleware.

```
import * as csurf from 'csurf';
// ...
// somewhere in your initialization file
app.use(csurf());
```

Use with Fastify

Start by installing the required package:

```
$ npm i --save @fastify/csrf-protection
```

Once the installation is complete, register the `@fastify/csrf-protection` plugin, as follows:

```
import fastifyCsrf from '@fastify/csrf-protection';
// ...
// somewhere in your initialization file after registering some storage
plugin
await app.register(fastifyCsrf);
```

> warning **Warning** As explained in the `@fastify/csrf-protection` docs here, this plugin requires a storage plugin to be initialized first. Please, see that documentation for further instructions.