Servant and XSS/CSRF

This is very quick

Cyrill Brunner

3rd October 2022

What will I show you?

- CSRF Protection with `servant-auth(-server)`

What will I show you?

- CSRF Protection with `servant-auth(-server)`
- XSS Protection with `shakespeare`

CSRF

```
type API = ...


server :: Server API

main = do
  ...









  run 8080 $ serve
    (Proxy :: Proxy API)

    server
```

CSRF

```
type API = ...

type SecuredAPI = Auth '[Cookie] LoginToken :> API
securedServer :: Server SecuredAPI

main = do
  ...









  run 8080 $ serve
    (Proxy :: Proxy SecuredAPI)

    securedServer
```

CSRF

```
type API = ...

type SecuredAPI = Auth '[Cookie] LoginToken :> API
securedServer :: Server SecuredAPI

main = do
  ...

  run 8080 $ serveWithContext
    (Proxy :: Proxy SecuredAPI)
    (jwtSettings :. cookieSettings :. EmptyContext)
    securedServer
```

CSRF

```
type API = ...

type SecuredAPI = Auth '[Cookie] LoginToken :> API
securedServer :: Server SecuredAPI

main = do
  ...

  xsrfCookieSettings = def { xsrfExcludeGet = True }









  run 8080 $ serveWithContext
    (Proxy :: Proxy SecuredAPI)
    (jwtSettings :. cookieSettings :. EmptyContext)
    securedServer
```

CSRF

```
type API = ...

type SecuredAPI = Auth '[Cookie] LoginToken :> API
securedServer :: Server SecuredAPI

main = do
  ...

  xsrfCookieSettings = def { xsrfExcludeGet = True }
  cookieSettings
    = def { cookieXsrfSetting = Just xsrfCookieSettings
          , cookieMaxAge = Just (60 * 60 * 24 * 7) -- 7 days
          }



  run 8080 $ serveWithContext
    (Proxy :: Proxy SecuredAPI)
    (jwtSettings :. cookieSettings :. EmptyContext)
    securedServer
```

CSRF

```
type API = ...

type SecuredAPI = Auth '[Cookie] LoginToken :> API
securedServer :: Server SecuredAPI

main = do
  ...

  xsrfCookieSettings = def { xsrfExcludeGet = True }
  cookieSettings
    = def { cookieXsrfSetting = Just xsrfCookieSettings
          , cookieMaxAge = Just (60 * 60 * 24 * 7) -- 7 days
          }

  jwtSettings = ...

  run 8080 $ serveWithContext
    (Proxy :: Proxy SecuredAPI)
    (jwtSettings :. cookieSettings :. EmptyContext)
    securedServer
```

XSS

XSS Protection is the default in Shakespeare!

XSS - Hamlet

```
handle userInput = do
  ...

  pure [shamlet|
    <p>You gave us: #{userInput}
    <p>Without interpolation: #{preEscapedToMarkup userInput}
  |]
```

XSS - Cassius

```
pure $ [cassius|
  .page-container
    background-color: #{userThemeColor}
    h1
      font-size: #{userThemeFontSize}


|] undefined
```

XSS - Lucius

```
pure $ [lucius|
  .page-container {
    background-color: #{userThemeColor}
    h1 {
      font-size: #{userThemeFontSize}
    }
  }
|] undefined
```

XSS - Julius

```
pure $ [julius|
  const userPreferences = JSON.parse("#{userPreferences}");
  document
    .querySelector(".#{rawJS greetingClassName}")
    .textContent = userPreferences.personalGreeting;
|] undefined
```