How to Harden Your Application

- Enable Twofactor SMS authentication
- Hardening Tomcat

Enable Twofactor SMS authentication

Understanding two factor authentication

Two factor security will require authenticated user to

1. Provide a passcode sent to their cell phone
2. Login from one the office IP addresses ("Office IP")
3. Login from an IP that they have succesfully logged in from X times before ("Home IP")

The IP based requirements are optional, and HomeIP is a subset of the OfficeIP solution.

Note: This functionality is still considered BETA

Preparation

To enable 2 factor authentication for users you will need to prepare the following:

- List of IP's that should not require 2 factor authentication
- An messaging URL for sending SMS's

Optionally you will also enter cellphone numbers for all employees in their user user profiles.

Step by step setup

System configuration

First you will setup the system to run in testmode, so that all messages are sent for you. After checking everything works, disable the testmode.

Change server configurations

- Set **smsConnectUrl** to your connection URL
- Check that **smsParamMessage** fits the parameter name of your SMS provider
- Check that **smsParamNumber** fits the parameter name of your SMS provider

Optionally you can allow IP based exceptions from the rules

- Set **passcodeTrustedIp** to true
- Set **passcodeTrustedIpList** to contain your office IP's

Furthermore you can allow multiple logins from the same IP to

- Set **passcodeUserIpHistory** to true
- Set **passcodeUserIpHistoryCount** to minimum succesfull logins

Activate passcode filters

Stop the application server

Go to the application folder and dive into: <application>\WEB-INF\web.xml

Uncomment the section containing the servlet mapping

```
<filter>
  <filter-name>TwoFactorAuthentication</filter-name>
  <filter-class>dk.tempusserva.passcode.SmsVerificationFilter</filter-class>
</filter>
<filter-mapping>
  <filter-name>TwoFactorAuthentication</filter-name>
  <url-pattern>/main</url-pattern>
</filter-mapping>
```

Start the application server

Test and go live

Validate that two factor login works as intended.

Change server configurations

- Set **smsTestMode** to false

Hardening Tomcat

Secure SSL ciphers

If you are running your Tomcat installation behind a reverse proxy, these recommendations will not be needed, as Tomcat is not terminating SSL/TLS.

Change the HTTP connector please use the following ciphers (<tomcat>\conf\server.xml)

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_GCM_SHA256
```

List updated: 2018-02-07

Secure headers

If you are running your Tomcat installation behind a reverse proxy, these recommendations will not be needed, as Tomcat is not terminating SSL/TLS.

In the SERVER web.xml (<tomcat>\conf\web.xml) uncomment the following sections

```
<filter>
  <filter-name>httpHeaderSecurity</filter-name>
  <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
  <async-supported>true</async-supported>
  <init-param>
    <param-name>antiClickJackingOption</param-name>
    <param-value>SAMEORIGIN</param-value>
  </init-param>
</filter>
```

```
<filter-mapping>
  <filter-name>httpHeaderSecurity</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

Additional CRSF filtering

The TS platform is already safe from CRSF attacks. CRSF tokens are generated at login and required for all data altering transactions.

The TS implementation does not use rotating or page specific CRSF tokens, so if additional security is needed use the OWASP implementation.

Additional security filters

Tempus Serva comes with multiple additional security features

- Lock user session to IP
- Lock service to listed countries
- Use passcode sent by SMS

The filters are activated by uncommenting the code in the applications /WEB-INF/web.xml.

Note that the filters can be set any part of the application: login, designer, webinterface and rest.

Validating your site

You can use the following services to check the security of your installation

Test SSL

Tip: Remember to check "Do not show the results on the boards"

https://www.ssllabs.com/ssltest/

https://sikkerpånettet.dk/

Test Headers

https://tools.geekflare.com/report/header-security-test