Universidade do Minho

Mestrado em Engenharia Informática

Engenharia de segurança

Ficha de exercício 8

Grupo 1

Rui Carlos Azevedo Carvalho - PG47633
Daniel Barbosa Miranda - PG47123
Ana Luísa Lira Tomé Carneiro - PG46983

Secure Software Development Lifecycle (S-SDLC)

Pergunta P1.1

Exercício 1

O regulamento RGPD deve ser levado em conta na função "Governance" e prática de segurança "Policy & Compliance" dado que esta consiste na aprendizagem de regulamentação legal externa ao sistema de forma a cumprir requisitos obrigatórios dessa natureza. A atividade que promove a introdução do RGPD é a que está presente na *stream B* que indica que devem ser identificados requisitos de entidades terceiras e que estes devem ser levados em consideração [2].

Exercício 2

A empresa tem de estar no nível de maturidade 1, dado que neste nível, é indicado pela *stream B* que devem ser identificados requisitos de terceiros e que estes devem ser levados em conta para as políticas que a empresa adotou de forma *standard* [2].

Pergunta P1.2

Exercício 1

No âmbito da realização do PD1, foram utilizadas diversas bibliotecas ou APIs *open source* de forma a conseguir implementar o projeto pretendido. Assim forma utilizadas as bibliotecas de python **sys**, **socket**, **os**, **pickle**, **threading**, **cryptography** e **pycryptodome**. As primeiros 5 bibliotecas apresentadas fazem todas parte integrante da linguagem python, ou seja, ao instalar o python esta bibliotecas vêm incluídas na instalação. Desta forma, cada uma destas bibliotecas possui a mesma versão e licença que a versão do python utilizada, ou seja, estas 5 bibliotecas encontram-se na versão 3.9.10, pois esta foi a versão do python utilizada para implementar o projeto. No que toca à licença destas bibliotecas, esta encontra-se descrita no seguinte link. No caso do módulo socket, para além da licença apresentada acima como esta biblioteca implementa as funções getaddrinfo e getnameinfo, que são codificadas num ficheiro em separado pertencente ao WIDE Project, esta biblioteca também apresenta a seguinte licença[1].

```
Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.
```

```
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.
```

No caso do cryptography, como é necessário a instalação desta biblioteca aparte do python, esta terá uma versão e licença distintas da linguagem. Para o caso do projeto PD1, foi utilizado a versão 36.0.1 desta biblioteca que possui a seguinte licença.

Finalmente, no caso da biblioteca pycryptodome esta tem uma utilização semelhante ao cryptography tendo por isso uma versão e uma licença distintas do python. No projeto PD1 foi utilizada a versão 3.4.6 da biblioteca, sendo a licença encontra descrita no seguinte link

Exercício 2

Segundo a licença do python apresentada, que influência na utilização das bibliotecas, sys, socket, os, pickle e threading, é possível a um utilizador destas bibliotecas reproduzir, analisar, testar, correr, exibir publicamente e distribuir o código apresentado nestas bibliotecas. Visto que todas as bibliotecas são *openSource*, para as distribuições que alteram o código original é necessário que o utilizador apresente um sumário das alterações feitas para que os restantes utilizadores que utilizam a sua distribuição tenham conhecimento de tal, sendo que a licença do python deixa de ser viável caso isto não aconteça. Contudo, não é permitido aos utilizadores utilizarem *trademarks* e *trade names* do PSF (Python Software Foundation) para uso publicitário, apoio financeiro e promoção de produtos e serviços do PSF. Todos os utilizadores que copiam, instalam ou usam o python estão a concordar com estes termos.

Para o caso particular da biblioteca socket para além desta vinculada pelas permissões e impedimentos presentados esta também tem permissões particulares para quando o utilizador utiliza as funções getaddrinfo e getnameinfo. Para estas funções é permitido que o utilizador redistribua o código com ou sem alterações, contudo é necessário que esta redistribuição seja feita segundo certas limitações. Umas das condições passa por evidenciar nas redistribuições em *source code* a licença vinculada ao código, reprodução da licença em caso de redistribuição de código binário e os nomes do projeto ou dos contribuidores do projeto não devem ser usados para promover e vender produtos sem antes pedir permissão aos lesados.

No caso da biblioteca cryptography esta licença é semelhante à apresentada pelo o python sendo por isso permitido aos utilizadores reproduzir, analisar, testar, correr, exibir publicamente e distribuir o código apresentado nesta biblioteca. É também obrigatório que utilizadores que distribuam código alterado desta biblioteca apresentem um sumários das alterações realizadas para que todos os utilizadores tomem conhecimento de tal. De resto, não é permitido aos utilizadores utilizarem *trademarks* e *trade names* do PSF (Python Software Foundation) para uso publicitário, apoio financeiro e promoção de produtos e serviços do PSF.

Finalmente, para o caso do pycryptodome, todos os utilizares estão livres de copiarem, modificarem, publicarem, usarem, compilarem, venderem e/ou distribuírem software que use esta biblioteca em *sorce code* ou em formato binário para uso comercial ou não. Contudo, nestas distribuições é necessário que os utilizadores apliquem certas restrições como evidenciar em *source code* a licença vinculada ao código e a reprodução da licença em caso de distribuição de código binário.

Exercício 3

No caso desenvolvimento de código *open source* que pode ser modificado e utilizado por diversos utilizadores é sempre correto declarar todas as licenças de bibliotecas externas utilizadas que estejam vinculadas ao projeto e versões de controlo de forma a que todos os utilizadores tenham conhecimento das versões de bibliotecas que correm no programa. Caso haja necessidade de alteração de uma funcionalidade de uma determinada biblioteca é sempre importante que esta alteração esteja documentada e que seja evidenciado que houve necessidade de alteração dessa funcionalidade. Todo código que seja copiado deve ser ser documentado com o link ou informação de onde foi retirado e devemos sempre seguir as *guidelines* apresentadas nas licenças. Caso estejamos a usar uma biblioteca que seja redistribuída e que por isso não seja a original é necessário ter em atenção se cumpre com os *guidelines* obrigatórios e se se encontra bem documentada para facilitar a sua utilização no projeto.

Bibliography

[1] "History and License" [online]. Disponível em: https://docs.python.org/3/license.html [Acedido em maio de 2022].

[2] "Policy & Compliance" [online]. Disponível em: https://owaspsamm.org/model/governance/policy-and-compliance/ [Acedido em maio de 2022]