Entreguem no formato PDF com as respectivas respostas.

Nome:

Turma:

E-mail corporativo:

1. Quais são os 3 tipos de ataques de XSS? Na interpretação do ataque qual deles é o que mais traz risco e por quê? Se possível escreva um trecho de “**pseudocódigo**” que resolva esse problema.
2. Podemos afirmar que o Diffie Hellman serve para autenticação? Por quê?
3. Descreva com suas palavras e como compreendeu o tema apresentado “Ciclo de Desenvolvimento de Software Seguro”.
4. Qual foi a motivação para criação do PCI?
5. Qual dos controles do PA é mais próximo as questões de desenvolvimento de código? (Ex.: PA 3.X)
6. ***“The Security Champions***“é uma forma de ampliação do time de S.I nas ***squads*** e times de tecnologia, porém existem algumas limitações recomendadas , e devem ser respeitadas, quais seriam essas recomendações citadas ?
7. Hash faz parte do contexto criptográfico, mas não é utilizado para criptografia, seguindo os conceitos básicos, explique por quê?
8. Ao desenhar a arquitetura de uma aplicação mobile, o ***P.O*** solicita o uso de biometria em um dispositivo móvel. Como você desenvolvedor ***back-end*** enxerga os riscos associados? Quais são os possíveis controles mitigatórios recomendados?
9. Na imagem abaixo qual tipo de vulnerabilidade está sendo demonstrada?

Utilizando o método de correção teórico, classifique, fazendo uso das calculadoras cvss, coloque o score e a string se possível.

Text

Description automatically generated

10) Em aplicações e arquitetura modernas o uso de Firewall, ou VPN são problemas de gestão na integração com os parceiros. Qual solução alternativa a esse processo, de exposição de API’S que dificultam o consumo não autorizado bem como o acesso e autenticação?

1. A imagem abaixo mostra um código, supostamente vulnerável. Identifique onde está e qual é a vulnerabilidade .Classifique usando o CVSS, proponha um trecho de código, caso queira pode se utilizar do ***gitpod***.

Text

Description automatically generated

1. Com base em alguns descritivos, modele alguns riscos/fraudes e proponha controles:

... “No meu e-commerce desejo dar aos clientes cashback nas transações realizadas pelo mesmo, com cartão e boleto e outros meios possíveis” ...

...” Desejo ofertar aos meus clientes i**tens promocionais exclusivos em e-commerce” ....**