H-CYBER APP

(SERVIÇO DE CONTROLO DE QUALIDADE E ANÁLISE DE VULNERABILIDADES AO CÓDIGO / APLICAÇÕES)

CYBER EFFECT - NÍVEL 2 - PROATIVO

DESCRIÇÃO

A Hardsecure tem um serviço que fornece a Revisão do Código de acordo com as melhores práticas de Cibersegurança, criado como um processo de auditoria do código fonte para aplicações e/ou base de dados. Permite verificar se os controlos de segurança estão adequados e atualizados, se funcionam como pretendido, e se estão a ser aplicados de forma correta. A nossa revisão ao Código/ Aplicações assegura que uma aplicação ou base de dados foi desenvolvida de modo a estar segura no seu ambiente de produção.

PROPOSTA DE VALOR

A revisão do código de Cibersegurança garantirá aos nossos clientes que os programadores de aplicações ou fornecedores de software estão a seguir técnicas e práticas de desenvolvimento seguras.

A nossa equipa utilizará o Threat Modelling para analisar a segurança de uma aplicação. É uma abordagem estruturada que permite ao cliente identificar, quantificar e abordar os riscos de segurança associados a uma aplicação ou base de dados. O Threat Modelling não é uma abordagem à revisão de código, mas complementa o processo de revisão do código de segurança. A inclusão do Threat Modelling no SDLC, ajudará a assegurar que as aplicações são/estejam a ser desenvolvidas com a segurança incorporada desde o início.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa
www.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER APP

(SERVIÇO DE CONTROLO DE QUALIDADE E ANÁLISE DE VULNERABILIDADES AO CÓDIGO / APLICAÇÕES)

CYBER EFFECT - NÍVEL 2 - PROATIVO

CARACTERÍSTICAS DO SERVIÇO

- **Utilização de quatro técnicas para análise da segurança de uma aplicação/software:** scanning automático, teste de intrusão manual, análise estática e revisão manual do código.

- **Revisão do código seguro concederá ao cliente o seguinte:** Autenticação, Autorização, Gestão da Sessão, Validação dos dados, Tratamento de erros, Registo e Encriptação.

- **Apoiar os clientes a criar modelos de ameaça, durante a fase de conceção**, educando os programadores sobre práticas seguras de programação (formação) e realizando frequentes revisões de código por pares com a equipa de segurança Hardsecure Pentest e OWASP, aumentando a qualidade geral do código e reduzindo o número de problemas reportados (e que precisam de ser corrigidos) pela revisão segura do código.

VALOR ACRESCENTADO

» Compreendemos a abordagem dos programadores. Antes de iniciar uma revisão segura do código, falamos com os programadores dos nossos clientes para compreender as suas abordagens a mecanismos como a autenticação e validação dos dados. A informação recolhida durante esta discussão ajudará a iniciar a revisão e diminuirá significativamente o tempo que o nosso auditor passa a tentar compreender o código.

» Utilizamos múltiplas técnicas (técnicas manuais e automatizadas) para a revisão, porque cada método encontrará elementos ou findings que o outro não encontra. Além disso, utilizamos mais do que uma ferramenta automatizada, porque os pontos fortes de cada uma diferem e complementam as outras.

» Não avaliamos o nível de risco. A nossa revisão segura do código não tenta fazer julgamentos sobre o que é um risco aceitável. A nossa equipa de auditoria de segurança reporta o que encontra. O cliente utiliza o plano de avaliação de risco aprovado pelo seu próprio programa para avaliar o risco e decidir se aceita ou não.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa
www.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER APP

(SERVIÇO DE CONTROLO DE QUALIDADE E ANÁLISE DE VULNERABILIDADES AO CÓDIGO / APLICAÇÕES)

CYBER EFFECT - NÍVEL 2 - PROATIVO

» Ao executar uma revisão manual, ganhamos uma compreensão do código como um todo, depois concentramos a revisão em áreas importantes, tais como funções que lidam com o login ou interações com uma base de dados. Além disso, alavancamos ferramentas automatizadas para obter detalhes sobre falhas específicas.

» Damos seguimento aos pontos de revisão. Após uma revisão, realizamos uma discussão de seguimento com a equipa de desenvolvimento para os ajudar a compreender o significado das conclusões e a forma de as abordar.

» Fazemos uma revisão segura do código e não apenas testes de intrusão. As nossas equipas de auditoria podem fazer pentest num software em execução ou em ambiente de qualidade (aqui mais intrusivo).

» A Hardsecure integra no seu trabalho, frameworks e standards como:

- OWASP Risk Rating Methodology.
- Source Code Analysis Tools (SAST/DAST).
- FAIR Information Risk Framework.
- Microsoft Threat Modeling (STRIDE and DREAD).
- DBSAT (Oracle Database Security Assessment).

» Categorizamos as vulnerabilidades de acordo com o Common Vulnerability Scoring System (CVSS) de forma a garantir a:

- Exploração da vulnerabilidade.
- Avaliação da probabilidade associada a cada finding.
- Avaliação da probabilidade associada ao vetor de ataque.
- Avaliação da probabilidade associada à vulnerabilidade de segurança.
- Combinação de vários fatores, entregando uma estimativa dos impactos técnicos e de negócio da sua instituição.
- Integração de vários fatores para calcular o risco na sua totalidade.
- Determinar as técnicas adequadas à mitigação ou correção da vulnerabilidade.

Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa
www.hardsecure.com
(+351) 218 278 126
geral@hardsecure.com

H-CYBER APP

(SERVIÇO DE CONTROLO DE QUALIDADE E ANÁLISE DE VULNERABILIDADES AO CÓDIGO / APLICAÇÕES)

CYBER EFFECT - NÍVEL 2 - PROATIVO

Fornecemos segurança e robustez para garantir:

- Verificação da segurança.
- Parametrização de consultas.
- Codificação de dados.
- Validação de todas as entradas.
- Implementação de controlos de identidade e autenticação.
- Implementação de controlos de acesso.
- Proteção dos dados.
- Implementação de Logs e deteção de intrusão.
- Análise da estrutura e framework de segurança e respetivas bibliotecas de suporte.
- Manipulação de erros e exceções.

PEDIDOS DE PROPOSTA / INFORMAÇÃO

Para informações adicionais ou mais esclarecimentos, por favor entre em contato através de um dos seguintes meios:

Formulário "Hardsecure – Serviço de Controlo de Qualidade e Análise de Vulnerabilidades ao Código / Aplicações" (disponibilizado na página do serviço no website)

Comercial da Hardsecure:
(+351) 218 278 126
geral@hardsecure.com

Website:
www.hardsecure.com (Formulário **"Solicitar Proposta"**)