OWASP top 10 & OWASP proactive controls

Trabalho realizado por:

João Amorim a74806

João Rodrigues pg52787

Sérgio Ribeiro pg54708

OWASP Top 10

- Representa um padrão de excelência para a identificação de riscos de segurança.
- A elaboração baseia-se na análise de dados provenientes de uma série de fontes.
- Ajuda a promover uma cultura de desenvolvimento de software que dê prioridade à segurança.
- As organizações podem fortalecer as suas defesas contra ataques cibernéticos.

Riscos A1 & A10

Capital One Cyber Incident

A1:2021 – Broken Access Control

- Sistemas de controlo de acesso mal implementados.
- Falhas na divulgação não autorizada de informações.

A10:2021 – Server-Slide Request Forgery

- Induz o servidor a realizar pedidos para um domínio;
- Consequências.

Riscos A2 & A3

A2:2021 – Criptographic Failures

- Proteção inadequada de informações;
- Uso incorreto ou ausência de criptografia;
- Consequências.

A3:2021 – Injection

- Falha perigosa e comum;
- Injeção de código malicioso;
- Vulnerabilidades nas validações ou no tratamento inadequado de dados de entrada.

Risco A4

Equifax Data Breach

A4:2021 - Insecure Desing

- Falhas por meios de erros ou omissões no design;
- Equifax 2017 Data Breach;
- Prevenções.

Riscos A5 & A7

A5:2021 – Security Misconfiguration

- Apps configuradas inadequadamente;
- Causas;
- Prevenções

A7:2021 – Identification and Authentication Failures

- Falhas no processo de verificação de identidade dos utilizadores;
- Consequências;
- Exemplos de ataques;

Risco A6

Ransoware WannaCry

A6:2021 - Vulnerable and Outdated Components

- Uso de modulos desatualizados;
- Ransomware WannaCry 2017;
- A importância de manter sistemas atualizados.

Riscos A8 & A9

A8:2021 – Software and Data Integrity Failures

- Integridade do software ou dos dados não é verificada ou garantida;
- Causas;
- Consequências.

A9:2021 – Security Logging and Monitoring Failures

- Insuficiência de processos de registo e monitorização de sistemas.
- Causas;
- Prevenções/Mitigações.

OWASP Proactive Controls

- Integração de medidas de segurança desde o início do desenvolvimento
- Orientações para programadores com foco em segurança
- Estratégias preventivas para diminuir possíveis riscos

Controlos Proativos

C1: Define Security Requirements

- Identificação de requisitos de segurança desde o início do ciclo de vida do desenvolvimento.
- Análise de riscos para identificar ameaças específicas.
- Utilização de padrões e frameworks reconhecidos.

C2: Leverage Security Frameworks and Libraries

- Escolha de ferramentas confiáveis e com reputação de segurança.
- Manutenção e atualização regular das ferramentas.
- Personalização cuidadosa para atender aos requisitos específicos da aplicação.

Controlos Proativos

C3: Secure Database Access

- Utilização de consultas parametrizadas para evitar injeções SQL.
- Implementação de autenticação forte e autorização adequada.
- Cifragem de dados.
- Configuração de auditoria e monitorização para detetar atividades suspeitas.

C4: Encode and Escape Data

- Utilização de bibliotecas confiáveis de codificação e escape.
- Codificação na apresentação de dados para prevenir ataques XSS.
- Escape de dados em consultas SQL para proteção contra injeções.

Controlos Proativos

C5: Validate All Inputs

- Definição de critérios de validação para diferentes tipos de entrada.
- Implementação de validação no lado do servidor.
- Utilização de listas de permissão em vez de listas de exclusão.

C6: Implement Digital Identity

- Fortalecimento da autenticação com autenticação multifator.
- Gestão segura de sessões com timeouts e mecanismos de logout.
- Definição de políticas de senhas fortes.
- Proteção de dados de autenticação com hashing.

Controlos Proativos

C7: Enforce Access Controls

- Implementação de modelos de controle de acesso adequados.
- Aplicação do princípio do mínimo privilégio.
- Garantia de autenticação e autorização seguras para prevenir acessos não autorizados.

C8: Protect Data Everywhere

- Cifragem de dados em trânsito e em repouso.
- Gestão de chaves de cifragem.
- Mascaramento de dados e anonimização.
- Controlos de acesso a dados para garantir a segurança.

Controlos Proativos

C9: Implement Security Logging and Monitoring

- Definição de políticas de registo para eventos de segurança.
- Armazenamento seguro de registos.
- Análise contínua de registos de segurança.
- Integração com sistemas de resposta a incidentes.

C10: Handle All Errors and Exceptions

- Padronização de mensagens de erro.
- Revisão e monitorização de registos de erros.
- Testes de manipulação de erros durante o desenvolvimento.

Caso de estudo

2014 Target Data Breach

Contexto

- Invasores conseguiram acesso à rede da Target através das credenciais de um fornecedor
- Exploraram vulnerabilidades na infraestrutura de TI da empresa
- Dados foram roubados

Consequências

- Perda de confiança da parte do público
- Queda de vendas

Fim