Relatório de Pentest

Do resumo executivo à recomendação técnica: veja como uma entrega pode organizar riscos, evidências e próximos passos.

Modelo demonstrativo. Todos os ambientes, achados e resultados desta página são fictícios. Nenhum teste foi executado para produzir este exemplo. Ele não representa um cliente, uma auditoria concluída ou vulnerabilidades confirmadas.

RESUMO EXECUTIVO

Informação técnica para apoiar decisões.

Este modelo apresenta três situações hipotéticas em um laboratório. A apresentação distingue o cenário, o impacto potencial, a evidência ilustrativa e a recomendação. Em uma avaliação real, cada conclusão depende de evidência, revisão técnica e escopo autorizado.

2 ativos fictícios	**3** achados ilustrativos
1 prioridade alta ilustrativa	**DEMO** sem execução real

ESCOPO E OBJETIVOS

Um laboratório, sem alvos reais.

Ambiente fictício

- portal.example.test — aplicação web
- api.example.test — API de laboratório

Os endereços são identificadores ilustrativos. A página não envia requisições a esses ambientes.

Organização da avaliação

- Definição dos ativos, limites e autorização.
- Coleta de evidências e análise dos resultados.

- Validação, priorização e reteste de correções.

ACHADOS E EVIDÊNCIAS

Um registro claro para cada hipótese.

Severidades usadas apenas para ilustrar o formato. Não foram calculadas pontuações CVSS nem realizadas validações técnicas neste modelo.

DEMO-001

Alta · ilustrativa

Controle de acesso por objeto

Cenário fictício: uma conta de teste recebe um registro pertencente a outra conta do laboratório.

Impacto potencial

Em um cenário real, uma falha desse tipo poderia expor informações de outros usuários.

Evidência fictícia

```
Fixture ilustrativa: conta-exemplo-A → documento-exemplo-B
Resposta simulada: HTTP 200 · {"owner":"conta-exemplo-B"}
```

Recomendação

Validar no servidor a permissão da conta sobre cada objeto solicitado, além da autenticação da sessão.

Critério de reteste

Verificar que a conta A acessa seus próprios registros e recebe uma recusa ao solicitar os registros da conta B.

DEMO-002

Média · ilustrativa

Protocolos TLS legados

Cenário fictício: o inventário de configuração do laboratório indica suporte a TLS 1.0 e TLS 1.1.

Impacto potencial

Protocolos legados podem reduzir a proteção das conexões, conforme as configurações e os clientes utilizados.

Evidência fictícia

```
Fixture ilustrativa de configuração
TLS 1.0: habilitado · TLS 1.1: habilitado · TLS 1.2: habilitado
```

Recomendação

Planejar a desativação dos protocolos legados e manter versões e configurações adequadas às necessidades do ambiente.

Critério de reteste

Confirmar que os protocolos antigos são recusados e que os clientes necessários continuam funcionando.

DEMO-003

Baixa · ilustrativa

Política de conteúdo ausente

Cenário fictício: uma resposta HTML do portal de laboratório não inclui Content-Security-Policy.

Impacto potencial

A ausência dessa camada de proteção pode ampliar o impacto de outras falhas, dependendo da aplicação.

Evidência fictícia

```
Fixture ilustrativa de resposta HTTP
Content-Type: text/html · Content-Security-Policy: ausente
```

Recomendação

Definir uma política adequada à aplicação, avaliar seu efeito em modo de relatório e acompanhar as violações antes da adoção.

Critério de reteste

Verificar a presença da política e testar os recursos legítimos da aplicação. A ausência do cabeçalho, isoladamente, não confirma XSS.

PLANO DE REMEDIAÇÃO

Da evidência ao acompanhamento.

Priorizar

Em um trabalho real, considerar exposição, impacto, contexto de negócio e confiança na evidência antes de definir a ordem das correções.

Corrigir

Alinhar responsáveis e prazos, implementar as medidas acordadas e registrar as alterações realizadas.

Retestar

Reproduzir a verificação autorizada e documentar se o comportamento inseguro foi corrigido, persiste ou exige nova análise.

METODOLOGIA E LIMITAÇÕES

Transparência sobre o que foi avaliado.

Este exemplo aproveita a organização de um relatório fornecido como referência, substituindo os dados por cenários fictícios. Não utiliza o nome, os alvos ou as evidências do documento original.

Uma entrega real deve registrar o que foi executado, o que falhou e o que ficou pendente. Observações de configuração e hipóteses não devem ser apresentadas como explorações confirmadas. A profundidade e a cobertura dependem do escopo e das condições de execução.