{{NOME/EQUIPE}}

Relatório de Vulnerabilidades

{{NOME DO SITE}}

{{DATA}}

INFORMAÇÃO CONFIDENCIAL

ÍNDICE

INTRODUÇÃO

OBJETIVO

Este relatório foi elaborado com o intuito de identificar, analisar e catalogar vulnerabilidades envolvidas nos domínios e servidores da {NOME DO Site}, levando-se em conta a integridade, confidencialidade e disponibilidade das informações. Foi feita a classificação e organização dos problemas encontrados, como também as possíveis abordagens iniciais para a resolução.

METODOLOGIA

Foram usadas metodologias e recomendações de órgãos internacionais especializados em segurança da informação para a obtenção dos riscos envolvidos em todas as operações de TI.

Para a catalogação e verificação de riscos em Aplicações Web e Servidores foi utilizado o padrão OWASP.

A primeira intervenção foi feita segundo a metodologia Black Box, em que é simulada a abordagem de um atacante externo à aplicação. Foram utilizados diversos softwares especializados em testes de intrusão e verificações manuais em todos os pontos críticos do sistema.

FERRAMENTAS UTILIZADAS

SUMÁRIO EXECUTIVO

VISÃO GERAL DOS TESTES DE SEGURANÇA

TOTAL DE VULNERABILIDADES ÚNICAS				
10				
CRÍTICA	ALTA	MÉDIA	BAIXA	INFO
1	3	4	1	1
ZERO-DAY			EASILY-EXPLOITABLE	
0			5	

SUMÁRIO DOS TESTES

Início	Fim
{{DATA}}	{{DATA}}

TOTAL DE VULNERABILIDADE: 10

TOTAL DE VULNERABILIDADES DE SEVERIDADE CRÍTICA: 1

TOTAL DE VULNERABILIDADES DE SEVERIDADE ALTA: 3

TOTAL DE VULNERABILIDADE DE SEVERIDADE MÉDIA: 4

TOTAL DE VULNERABILIDADES DE SEVERIDADE BAIXA: 1

TOTAL DE VULNERABILIDADES INFORMACIONAIS: 1

TOTAL DE VULNERABILIDADES CORRIGIDAS: 0

TOTAL DE VULNERABILIDADES EM RETESTE: 0

TOTAL DE VULNERABILIDADES NÃO CORRIGIDAS: 10

ESCOPO DO PROJETO

1. {{NOME DO ESCOPO}}
2.

HISTÓRICO DE RETESTE

Nenhum reteste realizado.

VULNERABILIDADES

CRÍTICA

1. [NÃO CORRIGIDO] {{NOME DA FALHA}}
   - total de ativos afetados: 1 - corrigidas: 0 - reteste: 0 - não corrigidas: 1

ALTA

2. [NÃO CORRIGIDO] {{NOME DA FALHA}}
   - total de ativos afetados: 1 - corrigidas: 0 - reteste: 0 - não corrigidas: 1
3. [NÃO CORRIGIDO] {{NOME DA FALHA}}
   - total de ativos afetados: 1 - corrigidas: 0 - reteste: 0 - não corrigidas: 1
4. [NÃO CORRIGIDO] {{NOME DA FALHA}}
   - total de ativos afetados: 1 - corrigidas: 0 - reteste: 0 - não corrigidas: 1

MÉDIA

5. [NÃO CORRIGIDO] {{NOME DA FALHA}}
   - total de ativos afetados: 1 - corrigidas: 0 - reteste: 0 - não corrigidas: 1
6. [NÃO CORRIGIDO] {{NOME DA FALHA}}
   - total de ativos afetados: 1 - corrigidas: 0 - reteste: 0 - não corrigidas: 1
7. [NÃO CORRIGIDO] {{NOME DA FALHA}}
   - total de ativos afetados: 1 - corrigidas: 0 - reteste: 0 - não corrigidas: 1
8. [NÃO CORRIGIDO] {{NOME DA FALHA}}
   - total de ativos afetados: 1 - corrigidas: 0 - reteste: 0 - não corrigidas: 1

BAIXA

9. [NÃO CORRIGIDO] {{NOME DA FALHA}}
   - total de ativos afetados: 1 - corrigidas: 0 - reteste: 0 - não corrigidas: 1

INFO

10. [NÃO CORRIGIDO] {{NOME DA FALHA}}
    - total de ativos afetados: 1 - corrigidas: 0 - reteste: 0 - não corrigidas: 1

VULNERABILIDADE

SEVERIDADE

1. Nome

CRÍTICA

DESCRIÇÃO

CENÁRIO DE ATAQUE

RECOMENDAÇÃO

ATIVOS AFETADOS

- {{ESCOPO}}

VULNERABILIDADE

2. Nome

SEVERIDADE

ALTA

DESCRIÇÃO

CENÁRIO DE ATAQUE

RECOMENDAÇÃO

ATIVOS AFETADOS

- {{ESCOPO}}

VULNERABILIDADE

3. Nome

SEVERIDADE

ALTA

DESCRIÇÃO

CENÁRIO DE ATAQUE

RECOMENDAÇÃO

ATIVOS AFETADOS

- {{ESCOPO}}

VULNERABILIDADE

4. Nome

SEVERIDADE

ALTA

DESCRIÇÃO

CENÁRIO DE ATAQUE

RECOMENDAÇÃO

ATIVOS AFETADOS

- {{ESCOPO}}

VULNERABILIDADE

5. Nome

SEVERIDADE

MÉDIA

DESCRIÇÃO

CENÁRIO DE ATAQUE

RECOMENDAÇÃO

ATIVOS AFETADOS

- {{ESCOPO}}

VULNERABILIDADE

6. Nome

SEVERIDADE

MÉDIA

DESCRIÇÃO

CENÁRIO DE ATAQUE

RECOMENDAÇÃO

ATIVOS AFETADOS

- {{ESCOPO}}

VULNERABILIDADE

7. Nome

SEVERIDADE

MÉDIA

DESCRIÇÃO

CENÁRIO DE ATAQUE

RECOMENDAÇÃO

ATIVOS AFETADOS

- {{ESCOPO}}

VULNERABILIDADE	SEVERIDADE
8. Nome	MÉDIA

DESCRIÇÃO

CENÁRIO DE ATAQUE

RECOMENDAÇÃO

ATIVOS AFETADOS

- {{ESCOPO}}

VULNERABILIDADE

9. Nome

SEVERIDADE

BAIXA

DESCRIÇÃO

CENÁRIO DE ATAQUE

RECOMENDAÇÃO

ATIVOS AFETADOS

- {{ESCOPO}}

VULNERABILIDADE SEVERIDADE

10. Nome

INFO

DESCRIÇÃO

CENÁRIO DE ATAQUE

RECOMENDAÇÃO

ATIVOS AFETADOS

- {{ESCOPO}}

CONCLUSÃO

Após a meticulosa análise realizada pela **{{Nome da Equipe}}**, durante o período compreendido entre **{{Data de Início}}** e **{{Data de Final}}**, foram identificadas vulnerabilidades e configurações inseguras em **{{Nome do Site/Sistema}}** que podem impactar a **confidencialidade, integridade e disponibilidade** das informações e dos serviços. Caso não sejam tratadas de forma adequada, essas falhas podem ser exploradas por agentes maliciosos, resultando em **acesso não autorizado**, **exposição de dados**, **alteração indevida de informações**, **indisponibilidade do serviço** e impactos relevantes à reputação e conformidade da organização.

Os achados foram organizados por nível de severidade, permitindo uma priorização objetiva das correções. Recomenda-se que a equipe responsável trate inicialmente as vulnerabilidades de **criticidade Crítica e Alta**, uma vez que tendem a apresentar maior potencial de exploração e impacto. Em seguida, devem ser endereçados os itens de severidade **Média**, que frequentemente aumentam a superfície de ataque e podem viabilizar explorações encadeadas. Por fim, recomenda-se a correção dos achados de severidade **Baixa/Informacional**, visando reduzir vazamento de informações e fortalecer o endurecimento (hardening) do ambiente.

Como medidas gerais de mitigação, recomenda-se:

- Adotar **validação e saneamento de entradas** com abordagem por *whitelist* sempre que possível;
- Utilizar práticas seguras de desenvolvimento, incluindo **tratamento correto de saída** (encoding/escaping) e controles de sessão;
- Implementar mecanismos de **rate limiting**, políticas de senha robustas e, quando aplicável, **MFA**;
- Reforçar a camada de transporte com **configuração segura de TLS**, além de aplicar headers de segurança e ajustes de hardening;
- Melhorar **monitoramento e registros (logs)** para detecção e resposta a incidentes, com retenção e rastreabilidade adequadas.

Recomenda-se a definição de um plano de remediação com prazos e responsáveis, priorizando a correção das vulnerabilidades **Críticas (imediato)** e

Altas (curto prazo), seguidas das vulnerabilidades Médias (médio prazo) e, por fim, das vulnerabilidades Baixas/Informacionais (planejado), com realização de reteste após as correções.

A {{Nome da Equipe}} agradece a colaboração da equipe de {{Organização/Cliente}} e reforça a importância de manter uma postura contínua e proativa de segurança, garantindo a proteção dos ativos e a confiança dos usuários. Permanecemos à disposição para apoiar em futuras validações, revisões e melhorias no processo de segurança.

APÊNDICE: OVERVIEW EXPLICADO

Total de Vulnerabilidades Únicas	Resumo das vulnerabilidades únicas que foram identificadas durante os testes em relação aos itens dentro do escopo. Uma vulnerabilidade única é uma falha que pode ter várias instâncias, ou seja, vários alvos/ativos no escopo afetados pela mesma vulnerabilidade.
Vulnerabilidade Zero-Day	Zero-Day é uma vulnerabilidade que é desconhecida para o fornecedor, desenvolvedor e para sua organização. Esta falha de segurança é frequentemente explorada por hackers antes que o fornecedor, desenvolvedor ou sua organização tome conhecimento e se apresse para corrigi-la. Um ataque de Zero-Day pode incluir a infiltração de malware, spyware ou permissão de acesso indesejado a informações sensíveis ou confidenciais.
Vulnerabilidade facilmente explorável	Vulnerabilidades facilmente exploráveis são pontos fracos que geralmente são fáceis de detectar normalmente através do uso de ferramentas e scanners automatizados, possuem exploits públicos disponíveis e/ou não necessitam de muito esforço ou conhecimento técnico para sua exploração.
Vulnerabilidade de crítica prioridade	As vulnerabilidades nesta categoria podem levar a um impacto significativo na confidencialidade, integridade e/ou disponibilidade de sistemas e dados organizacionais se não forem tratadas imediatamente.
Vulnerabilidade de alta prioridade	As vulnerabilidades nesta categoria requerem atenção imediata e plano de ação.
Vulnerabilidade de média prioridade	As vulnerabilidades nesta categoria são menos urgentes, mas em algumas circunstâncias ainda podem representar uma ameaça ou consequência séria.
Vulnerabilidade de baixa prioridade	As vulnerabilidades nesta categoria não são uma ameaça iminente, mas devem ser mitigadas para evitar problemas a longo prazo.

APÊNDICE: DEFINIÇÃO DOS NÍVEIS DE SEVERIDADE

Severidade	Descrição
CRÍTICA Alta probabilidade de exploração nos próximos 12 meses	• Espera-se que o evento ocorra na maioria das circunstâncias • Probabilidade definida • Já aconteceu no passado e nenhuma forma de mitigação foi implementada • Inevitável - vai acontecer • Sem proteções adicionais, espera-se que o evento ocorra na maioria das circunstâncias
ALTA 50% de chance de exploração nos próximos 12 meses	• O evento provavelmente ocorrerá na maioria das circunstâncias • Com as proteções existentes, este evento provavelmente ocorrerá • Eventos como este têm ocorrido regularmente na indústria
MÉDIA 10% de chance de exploração nos próximos 12 meses	• O evento deve ocorrer em algumas circunstâncias • O evento ocorreu em diferentes setores
BAIXA 1% de chance de exploração nos próximos 12 meses	• O evento pode ocorrer em algumas circunstâncias • O evento não ocorreu na empresa, pode ocorrer em algumas circunstâncias

APÊNDICE: MAPEAMENTO DOS ATIVOS AFETADOS PARA CADA VULNERABILIDADE

1. Crítica - {{NOME}}
   - NÃO CORRIGIDO - {{ESCOPO}}

2. Alta - {{NOME}}
   - NÃO CORRIGIDO - {{ESCOPO}}

3. Alta - {{NOME}}
   - NÃO CORRIGIDO - {{ESCOPO}}

4. Alta - {{NOME}}
   - NÃO CORRIGIDO - {{ESCOPO}}

5. Média - {{NOME}}
   - NÃO CORRIGIDO - {{ESCOPO}}

6. Média - {{NOME}}
   - NÃO CORRIGIDO - {{ESCOPO}}

7. Média - {{NOME}}
   - NÃO CORRIGIDO - {{ESCOPO}}

8. Média - {{NOME}}
   - NÃO CORRIGIDO - {{ESCOPO}}

9. Baixa - {{NOME}}
   - NÃO CORRIGIDO - {{ESCOPO}}

10. Info - {{NOME}}
    - NÃO CORRIGIDO - {{ESCOPO}}

APÊNDICE: MAPEAMENTO DAS VULNERABILIDADES PARA CADA ATIVO AFETADO

1. {{ESCOPO}}
   - Crítica - NÃO CORRIGIDO - {{NOME}}
   - Alta - NÃO CORRIGIDO - {{NOME}}
   - Alta - NÃO CORRIGIDO - {{NOME}}
   - Alta - NÃO CORRIGIDO - {{NOME}}
   - Média - NÃO CORRIGIDO - {{NOME}}
   - Média - NÃO CORRIGIDO - {{NOME}}
   - Média - NÃO CORRIGIDO - {{NOME}}
   - Média - NÃO CORRIGIDO - {{NOME}}
   - Baixa - NÃO CORRIGIDO - {{NOME}}
   - Info - NÃO CORRIGIDO - {{NOME}}

APÊNDICE: PLANO DE AÇÃO

Severidade	Vulnerabilidade	Ação	Impacto
CRÍTICA	{{Nome}}	{{Açao}}	{{Impacto}}
ALTA	{{Nome}}	{{Açao}}	{{Impacto}}
ALTA	{{Nome}}	{{Açao}}	{{Impacto}}
MÉDIA	{{Nome}}	{{Açao}}	{{Impacto}}
BAIXA	{{Nome}}	{{Açao}}	{{Impacto}}

INFO	{{Nome}}	{{Açao}}	{{Impacto}}