RELATÓRIO DE TESTE DE INVASÃO

Pentest

Monitora

Contrato 37/2023

Agosto/2023

Teste

CONTROLE DE VERSÕES

Data	Versão	Autor	Observação
04/09/2023	**1**	**Adilson Rocha**	**Criacao do Documento**
05/09/2023	**1.1**	**Adilson Rocha**	**Revisao do Documento**
06/09/2023	**1.2**	**Adilson Rocha**	**Revisao do Documento**
07/09/2023	**1.3**	**Adilson Rocha**	**Revisao do Documento**

1. DIREITOS AUTORAIS

2. SEGURANÇA E CONFIDENCIALIDADE DE INFORMAÇÕES

Todas as informações fornecidas à Neotel relacionadas a esse documento serão tratadas com o mais absoluto sigilo e a mais rigorosa confidencialidade, de modo a evitar, por qualquer meio ou forma, o conhecimento do seu conteúdo por parte de terceiros. A obrigação de sigilo permanecerá válida pelo período em que o relacionamento comercial entre o Cliente e a Neotel perdurar.

Excluem-se do compromisso de confidencialidade aqui previsto as informações: (a) disponíveis ao público de outra forma que não por divulgação feita por qualquer das Partes ou por qualquer de seus representantes legais; (b) que comprovadamente já eram do conhecimento de uma ou de todas as Partes ou de qualquer de seus representantes, antes da referida Parte ou de seus respectivos representantes terem acesso às Informações Confidenciais em razão do presente Contrato; e (c) disponíveis ao público por meio da divulgação de informações relevantes e essenciais do Cliente, nos termos da legislação aplicável.

3. USO DE MARCAS

Todas as marcas registradas, logotipos, imagens e ilustrações utilizadas nessa proposta são de propriedade da Neotel Segurança Digital e de seus respectivos proprietários no Brasil e fora dele, e assim sendo, não podem ser usadas para qualquer propósito, sem permissão expressa.

4. OBJETIVO

Esse documento tem por objetivo apresentar resultados de teste de invasão (pentest), parte do serviço de Operação Assistida, item conforme item 8.5.12 do TR 01/2023.

5. LIMITAÇÕES DE ESCOPO DE RESPONSABILIDADE

6. Os resultados apresentados neste relatório representam a situação encontrada durante nossos levantamentos, no período compreendido de 05 de agosto a 20 de setembro, divididos em suas respectivas etapas, conforme detalhado em outros capítulos deste relatório e de acordo com os respectivos itens de escopo apresentados neste relatório, não considerando eventuais aspectos de controle ou fragilidades que eventualmente venham a ser manifestados após esse período.

Durante a execução dos trabalhos, não foram realizados testes de desempenho, de alta performance ou stress testing para aferição de métricas do tempo de resposta das aplicações ou recursos computacionais utilizados.

A NEOTEL não assegura nem assegurará o sucesso da implementação do resultado dos serviços, nem assegura ou assegurará que tal se verifique em nenhum prazo, tampouco responderá por eventuais oportunidades que deixem de ser identificadas, apresentadas ou exploradas, independentemente dos motivos ou das razões para tais ocorrências.

6. APLICAÇÃO ALVO

- URL: Monitora
- https://monitora.com.br

7. METODOLOGIA ADOTADA

A metodologia escolhida para o presente teste de invasão é a Blackbox, na qual o executor possui conhecimento mínimo sobre o Alvo, conduzindo as atividades em um ambiente externo, fora da rede do cliente.

A execução do pentest compreende os seguintes passos:

Id	Passo	Observação
1	**Descoberta**	**Realização de uma varredura de discovery, de natureza superficial, com o objetivo de catalogar arquivos, rotas e URLs que compõem a aplicação-alvo.**
2	**Varreduras**	**Realização de varreduras automatizadas com ferramentas proprietárias para identificar e classificar possíveis vulnerabilidades.**
3	**Análise**	**A partir das vulnerabilidades identificadas, realiza-se uma análise de seus resultados para identificar falsos-positivos e oportunidades de exploração.**
3	**Exploração**	**Conjunto de atividades direcionadas para obter sucesso na exploração de uma vulnerabilidade. Isso inclui ganho de acesso privilegiado a sistemas, arquivos ou dados, sequestro de sessão de usuários, entre outros.**
4	**Coleta de Evidências**	**Agrupamento de evidências, caso existam, que comprovem a exploração de vulnerabilidades.**
5	**Relatório**	**Elaboração de um relatório final contendo detalhes das explorações bem-sucedidas, evidências, vulnerabilidades encontradas e um histórico das atividades.**

8. MAPA DE IMPACTO

RISCO	IMPACTO NEGOCIAL	IMPACTO TECNOLÓGICO
Preencher	**Preencher**	**Preencher**

9. FERRAMENTAL UTILIZADO

Ferramenta	Versão	Finalidade
Nexpose	Cloud	Varreduras profundas por vulnerabilidades e exploits.
Metasploit	Cloud	Framework de exploração de vulnerabilidades, fuzzing, brute force
BurpSuite Professional	Cloud	Varreduras profundas por vulnerabilidades, exploits, fuzzing, repeater, intruder.
NMap	7.93	Portscanning, services discovery, vulnerabilidades e fuzzing.
SQLMap	Main GitHub	Varreduras, exploit e fuzzing de SQL-Injection em aplicações web.
Beef	Main GitHub	Varreduras, exploit e fuzzing de XSS(Cross-sitescripting)
Nexpose	Cloud	Varreduras profundas por vulnerabilidades e exploits.
Nexpose	Cloud	Varreduras profundas por vulnerabilidades e exploits.

10. MAPA DE IMPACTO

10.1. QUADRO DE SEVERIDADE

Nome	Critícas	Altas	Medias	Exploits	Atividades 90 dias
Monitora	0	0	2	0	0

10.2. RESUMO DE VULNERABILIDADES

ID	DESCRIÇÃO	RISCO	CVE / OWASP	OCORRÊNCIAS
0	Cross-site request forquery	Medio	A5	1

10.3. DETALHAMENTO DAS VULNERABILIDADES ENCONTRADAS

11. REMEDIAÇOES SUGERIDAS

Remediações gerais de segurança:

1. Aplicação de Patches de Segurança 1

- Preencher 1

- Preencher 2

2. Aplicação de Patches de Segurança 2

- Preencher 3

- Preencher 4

3. Aplicação de Patches de Segurança 3

- Preencher 5

- Preencher 6

4. Aplicação de Patches de Segurança 4

- Preencher 7

- Preencher 8

5. Aplicação de Patches de Segurança 5

- Preencher 9

- Preencher 10

6. Aplicação de Patches de Segurança 6

- Preencher 11

- Preencher 12

7. Aplicação de Patches de Segurança 7

- Preencher 13

- Preencher 14

8. Aplicação de Patches de Segurança 8

- Preencher 15

- Preencher 16

12. HISTÓRICO DE ATIVIDADES

ID	DATA	ATIVIDADE REALIZADA	ANALISTA
1	**04/08/2023**	**Reunião PMO - Aprovação do escopo**	**Adilson Rocha**
2	**04/08/2023**	**Reunião PMO - Aprovação do escopo**	**Adilson Rocha**

Adilson Rocha

Analista de Segurança NEOTEL

ANEXOS

DETALHAMENTO DE VULNERABILIDADES