



Laboratório Avançado de Produção Pesquisa e Inovação em Software

Escopo dos Testes de Penetração (Pentesting scope)

Red Team @ LAPPIS

Brasília, aos 5 de Agosto de 2024

1. Introdução

O presente documento consiste na definição de escopo dos testes de penetração que serão executados pelo time responsável pela segurança do projeto Brasil Participativo – BP composto atualmente por Rodolfo Cabral Neves, cujo objetivo é elucidar as atividades serão realizadas, os objetivos dos testes, os objetos em estudo ou *assets* que serão testados, metodologias análise de riscos e restrições bem como as suas limitações e necessidades.

2. Objetivo

O teste de penetração - *pentest* tem como objetivo descobrir e identificar **todas** as vulnerabilidades nos sistemas sob investigação e melhorar a segurança dos sistemas testados.

3. Metodologia

A abordagem utilizada nos testes será do tipo e *Black-Box* para a plataforma do Brasil Participativo – BP em ambiente local. Durante o processo de testes, serão utilizadas algumas ferramentas de automação e outros serão realizados de forma manual.

4. Escopo

Os testes terão os seguintes objetos:

1. Plataforma LAB-DECIDE (em ambiente local)

- Tipos de vulnerabilidades que se procura:
 - Cross-Site Scripting XSS
 - Insecure Direct Object References – IDOR
 - Information Disclosure
 - File Upload
 - Local File Inclusion
- Rotas:

- * (Todas as rotas da aplicação)

5. Limitações

Eis as atividades que **NÃO** serão realizadas durante o processo de testes:

- Alteração de qualquer arquivo configuração do servidor
- Alteração do código-fonte
- O teste de quaisquer elementos que não estão descritos no escopo

6. Prazos

Os testes serão conduzidos a partir do dia 6 de agosto de 2024 e terá duração de 2 semanas, podendo ser prorrogada de acordo a necessidades específicas.

Rodolfo Cabral Neves, líder do time de segurança do LAPPIS