**Projeto de Pentest no Sistema Sigaa**

**Grupo:**

Ana Carolina Rodrigues Lima de Aguiar - 20210024326

Cassiano Sabino - 20210025806

Geovana Maria dos Santos Lima - 20210024729

Victor Pessoa Oliveira Ortins - 20210024667

O intuito da proposta é realizar um Pentest, ou seja, um teste de penetração no sistema Sigaa, visando detectar prováveis vulnerabilidades em termos de segurança, capazes de comprometer a confidencialidade, a integridade e a disponibilidade dos dados. Para tanto, serão explorados quatro tipos de ataques usualmente empregados em um ambiente web, os quais podem ser atacados por invasores com poucos recursos técnicos:

**1. Buscas Específicas no Google:** Essa técnica, conhecida como Google Dorking, refere-se a desenvolvimento de buscas específicas no Google, com a finalidade de localizar arquivos sensíveis que possam ter sido expostos de forma indevida. Ou seja, proceder através de buscas que tentem localizar arquivos que contenham informações que possam ser logins e senhas do Sigaa ou do Moodle e que possam estar indexados em sua pesquisa.

**2. Ataque de Dicionário:** Visar testar combinações de login e senha utilizando matrículas dos novos alunos. A lógica seria que muitos deles ainda podem estar utilizando suas matrículas como senhas padrão, ou seja, não conseguiram mudar a sua senha no primeiro acesso, permitindo a exploração deste ataque por meio de tentativas automáticas de autenticação.

**3. Injeção SQL:** A injeção de SQL é um dos ataques mais comuns em aplicações web. Ela consiste em inserir um código SQL malicioso em um campo de entrada, como um formulário de login, com o intuito de influenciar as consultas ao banco de dados. Este tipo de ataque pode permitir acesso não autorizado a informações confidenciais ou até mesmo à manipulação de dados dentro do sistema.

**4. Varredura de Rede:** O objetivo da varredura de rede é mapear e identificar quais serviços vulneráveis estão sendo executados nos servidores do sistema Sigaa. Ela visa detectar portas abertas e serviços inseguros, que possam ser utilizados pelos invasores para obter acesso ao sistema ou a dados confidenciais.

Serão abordados esses quatro tipos de ataques para identificar possíveis vulnerabilidades no sistema Sigaa. O objetivo final é identificar essas vulnerabilidades de segurança e comunicar aos responsáveis para que sejam realizadas correções em tais vulnerabilidades.