



**Disciplina – *Segurança em Sistemas Computacionais***  
**Professor: *Carlos André Batista de Carvalho***

**Trabalho 01 – Implementação/Criptografia**

O OWASP Top 10 descreve as principais vulnerabilidades Web. Em sala, com base no livro “Segurança em Aplicações Web” da Casa do Código, foi abordado aspectos práticos sobre como testar se uma aplicação possui vulnerabilidades de SQL Injection e Cross-Site Scripting (XSS). Além disso, utilizamos a plataforma portswigger para aprender como realizar testes de segurança em um ambiente controlado.

Nesse contexto, a tarefa a ser executada, é detalhar o processo de e (cinco) testes de segurança diferentes, envolvendo pelo menos 3 vulnerabilidades distintas do OWASP Top 10. Não poderá ser incluindo nos testes, os experimentos realizados em sala (SQL Injection/ login bypass, XSS refletido/armazenado with nothing encoded). Os testes devem ser feito utilizando o portswigger. Posso aceitar outras plataformas, desde que comunicado previamente e autorizado.

**Deve ser gerado um relatório com os experimentos realizados que indiquem o passo a passo para a realização dos testes (ataques) e os resultados obtidos. A gravação de vídeos com os experimentos é bem vinda. Deve ser incluído no relatório uma breve descrição das vulnerabilidades, incluindo como o teste funciona e suas estratégias de mitigação (correção das vulnerabilidades).**