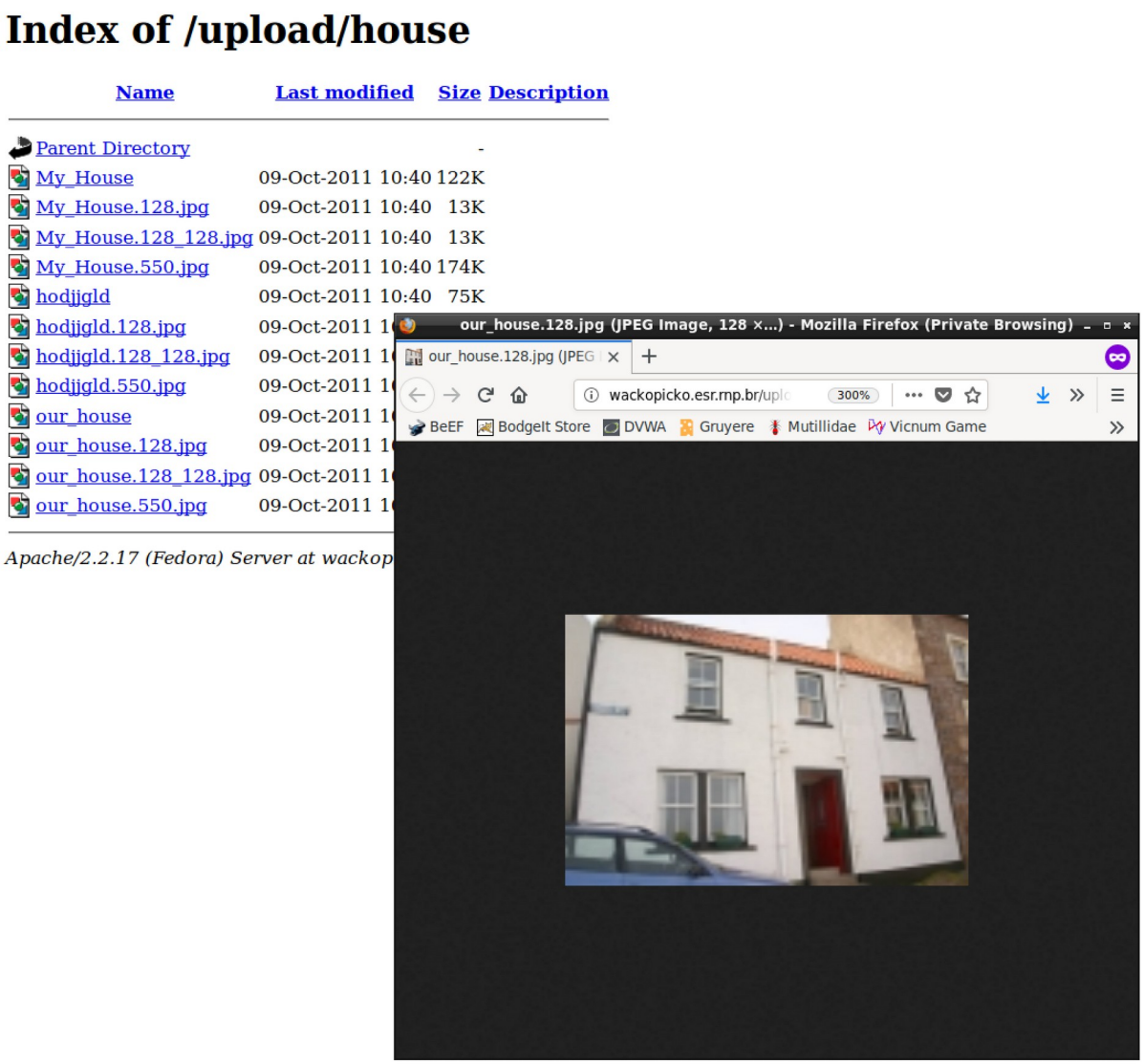
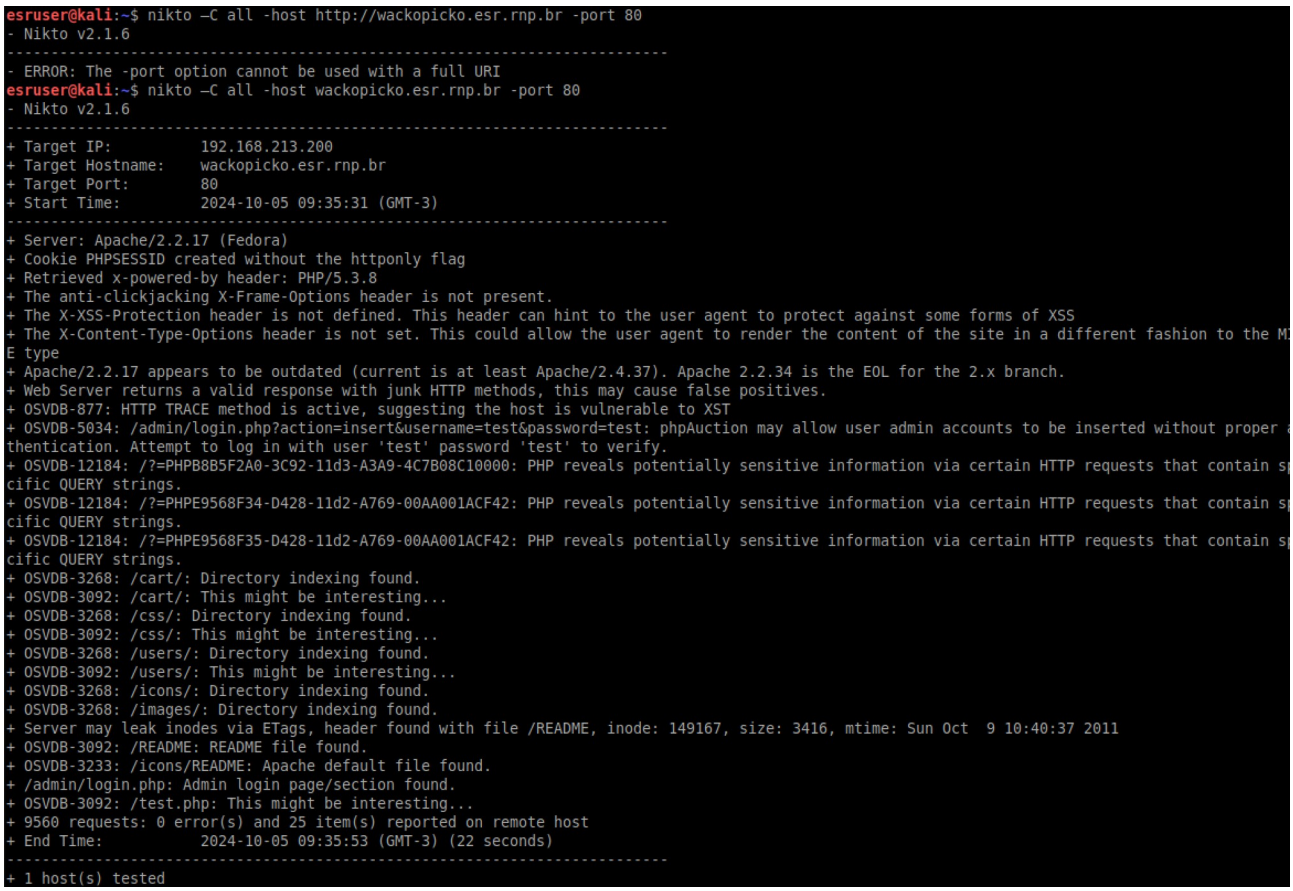
Atividade – Capture a bandeira

Demonstração de acesso direto a recursos e acesso ao sistema com usuário admin

A aplicação http://wackopicko.esr.rnp.br/ permite acesso sem autenticação aos recursos conforme a imagem abaixo.



Para simular esta vulnerabiliade, foi realizado login com os usuários cedidos e anotado as urls das postagens. Foi possível após o logout acessar os arquivos estáticos do sistema pois a navegação de diretórios está habilitada. Posteriormente executei a ferramenta nikto para ver se há vulnerabilidades comuns em servidores Web.



A análise detectou um arquivo README http://wackopicko.esr.rnp.br/README revelando várias informaçõe sensíveis como as credenciais de alguns usuários, entre eles os admins do sistema a qual foi possível obter acesso de administrador.