Sessão 10: Escrita de Relatórios e "Capture the Flag"

Atividade – Teste da aplicação Vicnum

Esta atividade tem por objetivo servir de aquecimento para o exercício de captura da bandeira, por meio da exploração de uma aplicação mais simples. Para iniciá-la, carregue as máquinas virtuais do aluno e do servidor (Fedora) e execute os roteiros na primeira delas.

O propósito desta atividade é descobrir as vulnerabilidades na aplicação Vicnum, que permitem que usuários trapaceiem no jogo e obtenham um resultado perfeito.

1. Inicie o Firefox, presente no menu Usual application\Internet.
2. Acesse http://vicnum.esr.rnp.br/
3. Entenda como funciona o jogo Vicnum, participando de algumas rodadas.
4. Execute o teste de invasão completo, para identificar as vulnerabilidades que permitem que alguns usuários trapaceiem.
5. Encerre o Firefox.

Atividade – Capture a bandeira

O objetivo desta atividade é exercitar todo o conhecimento adquirido neste curso, permitindo que o leitor realize um teste de invasão completo, em uma aplicação contendo diversos tipos de vulnerabilidades:

- Acesso direto a recursos (1x).
- Cross-site scripting (5x).
- Exposição de arquivos do sistema operacional (1x).
- Falha em lógica de negócio (1x).
- Identificadores de sessão previsíveis (1x).
- Inclusão de arquivos (1x).
- Injeção de comandos (1x).
- Injeção de SQL (2x).
- Manipulação de parâmetros (1x).
- Navegação de diretórios (1x).
- Revelação de informações (1x).
- Senha fraca (1x).
- Transporte inseguro de informações (2x).

Para acessar a aplicação, digite a seguinte URL em um navegador web: http://wackopicko.esr.rnp.br/

Algumas contas pré-cadastradas, que podem ser usadas, incluem:

- scanner1/scanner1.
- scanner2/scanner2.
- bryce/bryce.

A partir dessas informações, aplique a metodologia apresentada no Capítulo 2, baseada nas etapas de reconhecimento, mapeamento, descoberta de vulnerabilidades e exploração, e sucesso na realização da atividade!

ENTREGA DA TAREFA

Para que seja considerada entregue você deve anexar a esta atividade no AVA arquivo explicando, com o máximo de detalhes possível, um ataque utilizado contra o site que tenha obtido sucesso.

Última atualização 2020-07-27 11:29:41 -0300