UNIVERSIDADE REGIONAL DE BLUMENAU
CENTRO DE CIÊNCIAS EXATAS E NATURAIS
DEPARTAMENTO DE SISTEMAS E COMPUTAÇÃO
PROFESSOR GILVAN JUSTINO
SEGURANÇA DA INFORMAÇÃO

Lista de Exercícios 02

Para este exercício, compartilhe prints de telas do comando submetido.

1) Baixe o projeto UWAmp que está no exercício.

2) Descompacte o arquivo recém baixado numa pasta que não tenha espaços no nome. Por exemplo: c:\UWAmp

3) Abra o aplicativo UwAmp.exe que está dentro da pasta UwAmp
Apache e PHP devem ser iniciados. Caso ocorra falha, pode ser que a porta do Apache não esteja acessível, neste caso, clique no botão Apache Config e em "Virtual Server", selecione "Apache Main.." e altere à direita a porta (por exemplo: 9092). Repita para o endereço de exemplo também.

4) Clique no botão "www Site".

5) Localize o projeto "dvwa"

6) Na tela de login, utilizar:
Usuário: admin
Senha: password

7) No menu à esquerda, entre em "DVWA Security" e altere o nível de segurança para "Low".

Questão 1

Acesse a opção "Command injection" e tente explorar as vulnerabilidades abaixo. Coloque num documento os comandos que você usou e os prints das respostas que você obteve. Submeta este arquivo no AVA.

1 – Qual o IP do servidor?

2 – Qual é o usuário corrente do servidor?

3 – Qual o nome do diretório corrente?

4 – Com base na questão anterior, obtenha o conteúdo do arquivo "my.ini" que está no diretório "mysql". Suponha que a raiz do dispositivo não seja acessível pelo usuário da aplicação. Para isso, utilize o endereço relativo ao invés de endereço absoluto.

5 – Obtenha a lista de programas que estão em execução. Em seguida, publique esta lista no mesmo servidor, para que seja acessível na URL http://127.0.0.1:9090/saidas/programas.txt.

6 – Interrompa a execução do mysql