Tarefa realizada no dia: 19, 20 e 22/04

Representando a atividade**: Consulta Servidor - SQL Injection - SQL MAP**

Duração dos testes: 3 horas

Duração total da atividade: 3 horas e 30 min

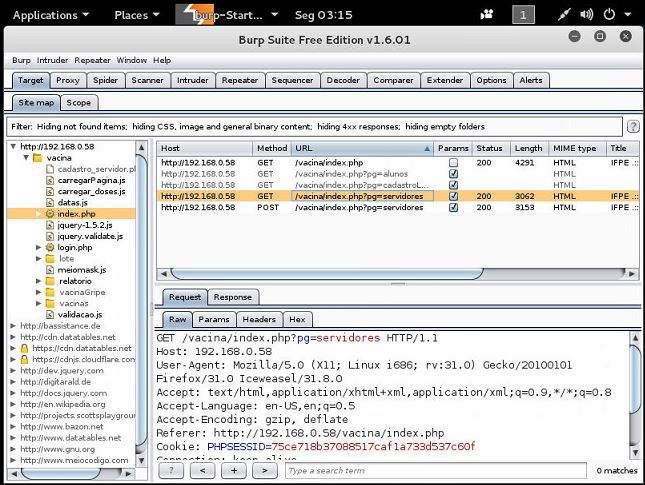
**Objetivo**: Utilizar a ferramenta SQL Map para automatizar o processo de detecção de vulnerabilidades na tela de Consulta Servidor a partir de injeção SQL.

**Resultados**:

**Tentativa 1:** Verificar se a tela de Consulta Servidor é vulnerável a injeção de código SQL e caso haja vulnerabilidade conseguir obter o nome do banco de dados utilizado pelo sistema.

Para realizar essa tentativa foi necessário utilizar o Burp Suite capturar as informações de cookie contidas no cabeçalho HTTP no momento em que a página do login é acessada.

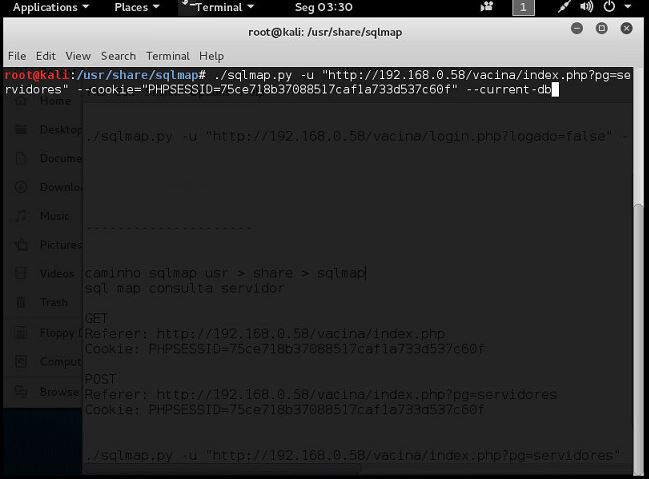
Parêmetros obtidos através do Burp Suite



Entrada:

./sqlmap.py -u "http://192.168.0.58/vacina/index.php?pg=servidores"

--cookie="PHSESSID=75ce718b37088517cafla733d53c60f" --current -db



**Resultado**: Passou no teste. Não possível encontrar vulnerabilidade na página e por consequência não foi possível descobrir o nome do banco de dados utilizado no sistema.

Segue abaixo algumas imagens evidenciando o scaneamento realizado pelo SQL Map.

**Tentativa 2:** Repetir a ação da tentativa 2 e aumentar o nível de heurística aplicado no escaneamento para o valor máximo: 5.

Entrada:

./sqlmap.py -u "http://192.168.0.58/vacina/index.php?pg=servidores"

--cookie="PHSESSID=75ce718b37088517cafla733d53c60f" --current -db --level 5

**Resultado**: Passou no teste. Mesmo aumentando o nível de heurística utilizado no escaneamento, não possível encontrar vulnerabilidade na página e por consequência não foi possível descobrir o nome do banco de dados utilizado no sistema.