Técnicas SQL Injection

O sqlmap é capaz de detectar e explorar cinco tipos diferentes de injeção de SQL:

Boolean-based blind: o sqlmap substitui ou anexa ao parâmetro afetado na solicitação HTTP uma string de instrução SQL sintaticamente válida contendo uma sub instrução SELECT ou qualquer outra instrução SQL cuja saída o usuário deseja recuperar. Para cada resposta HTTP, comparando os cabeçalhos/corpos da resposta HTTP com a solicitação original, a ferramenta infere a saída da instrução injetada caractere por caractere. Alternativamente, o usuário pode fornecer uma string ou expressão regular para corresponder às páginas True. O algoritmo de bissecção implementado no sqlmap para executar essa técnica é capaz de buscar cada caractere da saída com um máximo de sete solicitações HTTP. Quando a saída não estiver dentro do conjunto de caracteres simples de texto simples, o sqlmap adapta o algoritmo com intervalos maiores para detectar a saída.

Time-based blind: o sqlmap substitui ou anexa ao parâmetro afetado na solicitação HTTP uma string de instrução SQL sintaticamente válida contendo uma consulta que suspende o retorno do SGBD back-end por um determinado número de segundos. Para cada resposta HTTP, comparando o tempo de resposta HTTP com a solicitação original, a ferramenta infere a saída da instrução injetada caractere por caractere. Assim como na técnica baseada em booleanos, o algoritmo de bissecção é aplicado.

Error-based: o sqlmap substitui ou anexa ao parâmetro afetado uma instrução que provoca uma mensagem de erro específica do banco de dados e analisa os cabeçalhos e o corpo da resposta HTTP em busca de mensagens de erro do SGBD contendo a cadeia de caracteres predefinida injetada e a saída da instrução da subconsulta. Essa técnica funciona somente quando o aplicativo web foi configurado para divulgar mensagens de erro do sistema de gerenciamento de banco de dados back-end.

UNION query-based: o sqlmap anexa ao parâmetro afetado uma instrução SQL sintaticamente válida começando com UNION ALL SELECT. Essa técnica funciona quando a página do aplicativo web passa diretamente a saída da instrução SELECT dentro de um loop for ou similar, de forma que cada linha da saída da consulta seja impressa no conteúdo da página. O sqlmap também é capaz de explorar vulnerabilidades de injeção de SQL em consultas UNION parciais (entrada única), que ocorrem quando a saída da instrução não é ciclada em uma construção “for”, enquanto apenas a primeira entrada da saída da consulta é exibida.

Stacked queries: também conhecidas como “piggy backing”: o sqlmap testa se o aplicativo web suporta consultas empilhadas e, caso suporte, anexa ao parâmetro afetado na solicitação HTTP um ponto e vírgula (;) seguido pela instrução SQL a ser executada. Essa técnica é útil para executar instruções SQL diferentes de SELECT, como, por exemplo, instruções de definição ou manipulação de dados, possivelmente levando ao acesso de leitura e gravação do sistema de arquivos e à execução de comandos do sistema operacional, dependendo do sistema de gerenciamento de banco de dados back-end subjacente e dos privilégios do usuário da sessão.