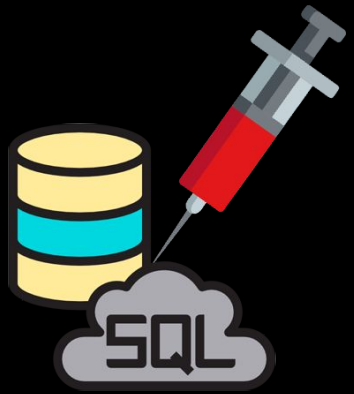
Inferential SQLi

Blind

Inferential SQLi (Blind)

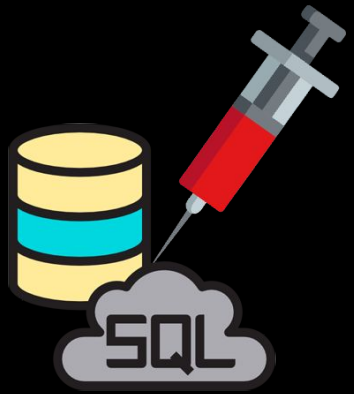


Inferential SQL Injection é o tipo de SQL Injection talvez mais comum e o mais muroso de explorar. Neste tipo de SQLi o resultado da nossa injeção não é mostrado diretamente pela aplicação web. Em vez disso, dependendo do resultado da query com a nossa injeção, a aplicação web vai comportar-se de forma diferente e, através da análise deste comportamento, podemos extrair informação do banco de dados.

As 2 técnicas mais conhecidas de In-Band SQL Injection são:

- Blind-Boolean-Based (Content-Based) SQLi
- Blind-Time-Based

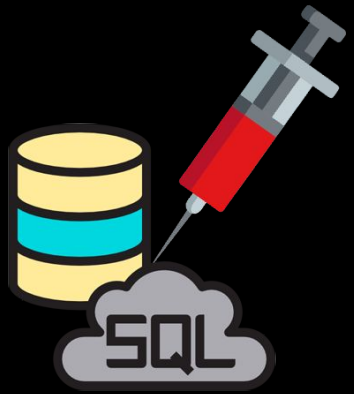
Blind-Boolean-Based (Content-Based)



Blind-Boolean-Based SQLi é uma técnica utilizada em vulnerabilidades do tipo Blind SQLi, que se baseia em enviar uma query SQL para o banco de dados que força a aplicação web a retornar resultados diferentes dependendo se a query devolve um resultado VERDADEIRO ou FALSO.

Dependendo do resultado VERDADEIRO ou FALSO da query, o conteúdo da resposta HTTP vai ser diferente ou permanecer o mesmo. Isto permite que um atacante / hacker consiga mapear toda a informação do banco de dados, embora demore muito mais tempo.

Blind-Time-Based



Blind-Time-Based SQLi é uma técnica utilizada em vulnerabilidades do tipo Blind SQLi, que se baseia em enviar uma query SQL para o banco de dados que força o banco de dados a esperar um tempo especificado antes de responder. O tempo de resposta irá indicar ao atacante /hacker se o resultado da query com a injeção SQL é VERDADEIRO ou FALSO.

Dependendo do resultado VERDADEIRO ou FALSO da query, o conteúdo da resposta HTTP vai ser retornada com um delay temporal ou imediatamente. Isto permite que um atacante / hacker consiga mapear toda a informação do banco de dados, embora demore muito mais tempo.