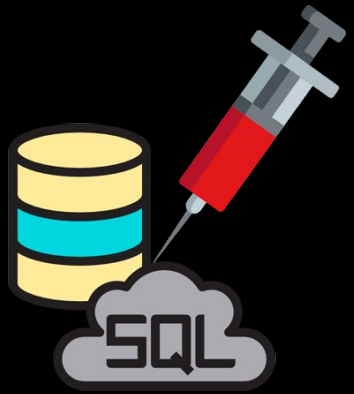
In-Band SQLi

Classic

In-Band SQLi (Classic)

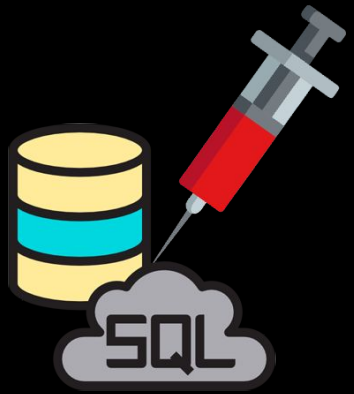


In-Band SQL Injection é o tipo de SQL Injection mais facil de explorar. Este tipo de SQLi acontece quando o atacante / hacker é capaz de utilizar o mesmo canal de comunicação para realizar o ataque e obter os respectivos resultado.

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

- Error-Based SQLi
- Union-Based SQLi

Error-Based SQLi

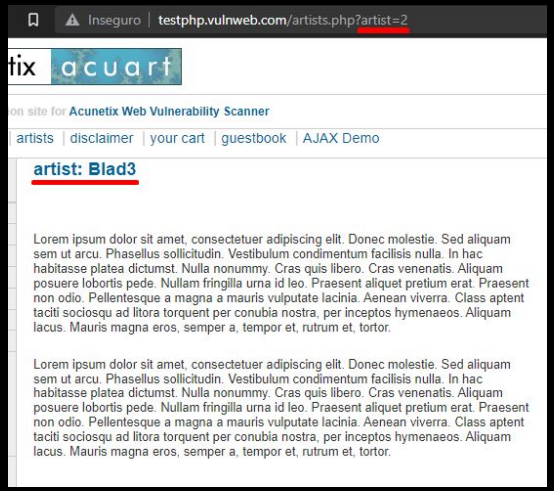


Error-Based SQLi é uma técnica utilizada em vulnerabilidades do tipo In-Band, que se baseia nas mensagens de erro enviadas pelo servidor do banco de dados para obter mais informação sobre a estrutura do banco de dados. Em alguns casos, esta técnica por si só é suficiente para um atacante / hacker enumerar todo o banco de dados.

Embora estas mensagens de erro sejam muito importantes na fase de desenvolvimento da aplicação web, estas devem ser desativadas quando o website é enviado para produção / disponibilizado para a internet.

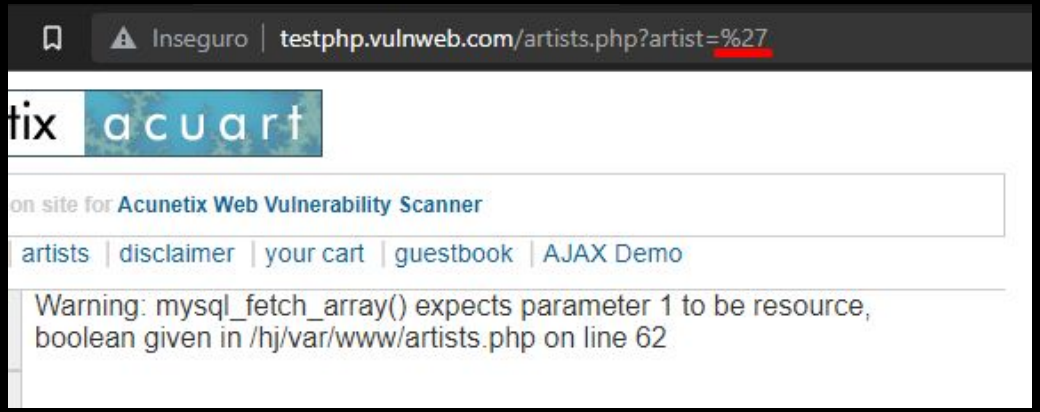
Error-Based SQLi - Exemplo

Neste exemplo verificamos que o website mostra a informação do artista cujo ID é o passado por parâmetro no URL da requisição:



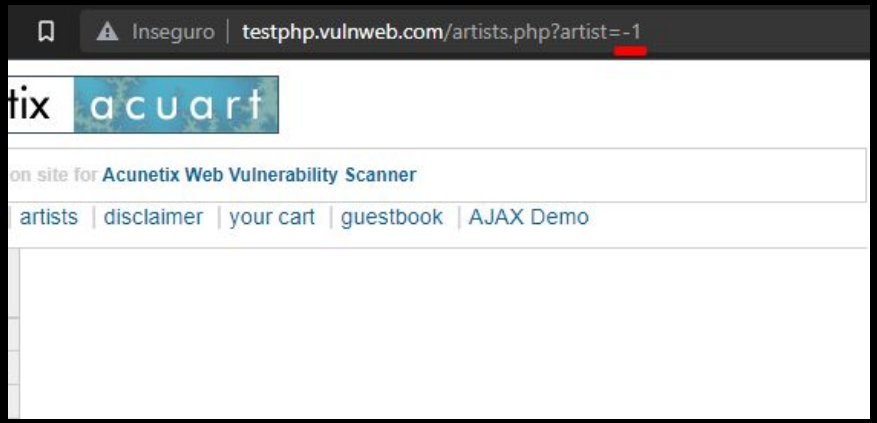
Error-Based SQLi - Exemplo

No entanto, se substituirmos o id do artista por um valor não válido, verificamos que o website mostra um erro SQL. Neste caso, substituímos o valor do ID por uma plica, que URL encoded corresponde a %27. Assim sendo, confirmamos que o input do usuário correspondente ao id do artista está a ser colocado diretamente na query SQL e está a gerar um erro, ou seja, descobrimos uma vulnerabilidade de SQL Injection.



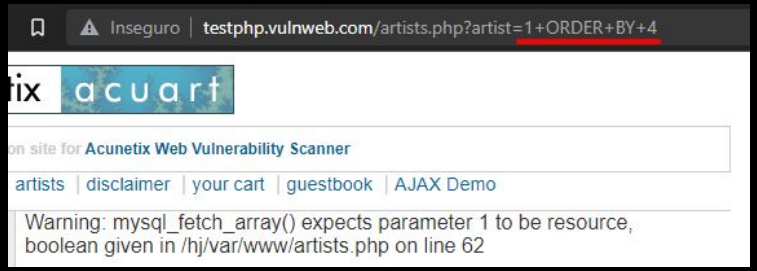
Error-Based SQLi - Exemplo

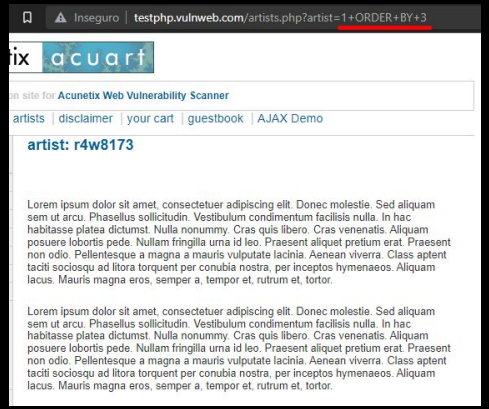
Através destes erros, podemos descobrir informação sobre o banco de dados. Se agora no id do artista colocarmos o valor -1, verificamos que não é mostrada nenhuma informação mas também não é gerado nenhum erro SQL. Isto acontece porque o valor -1 não gera nenhum erro SQL e, como não existe nenhum artista com id=-1, o resultado da query é "vazio".



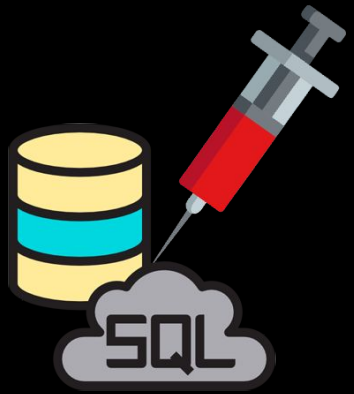
Error-Based SQLi - Exemplo

Sabendo isto, podemos agora manipular a query para saber, por exemplo, quantas colunas tem a tabela na qual está a ser feito o select com o id do usuário. Na primeira imagem é gerado um erro SQL porque estamos a tentar ordenar o resultado da query pela 4ª coluna e, a tabela não tem 4 colunas. Na segunda imagem, não verificamos a existência de um erro SQL o que significa que a tabela tem 3 colunas.





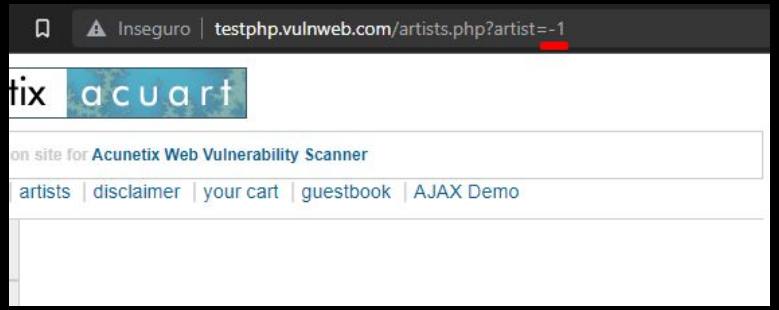
Union-Based SQLi

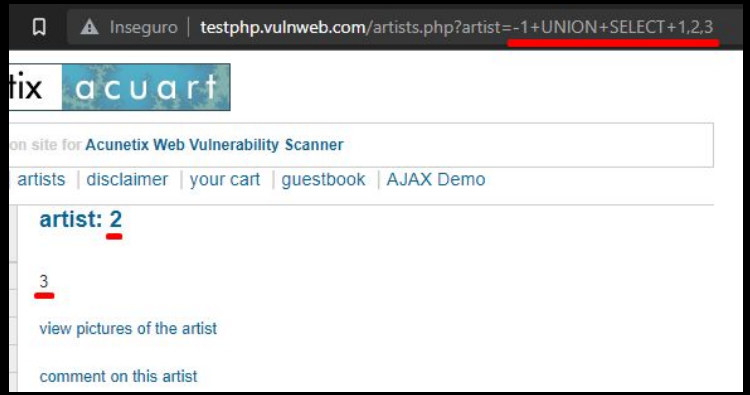


Union-Based SQLi é uma técnica utilizada em vulnerabilidades do tipo In-Band, que utiliza o operador SQL UNION para combinar o resultado de 2 ou mais SELECTs em um único resultado que é posteriormente devolvido como parte da resposta HTTP.

Union-Based SQLi - Exemplo

No mesmo exemplo, sabendo que a tabela na qual está a ser feito o SELECT com o id do artista tem 3 colunas, podemos usar o operador UNION para descobrir mais informação sobre o banco de dados. Vamos começar, por exemplo por descobrir qual é a coluna que está a ser mostrada pelo website. Neste caso, verificamos que é a coluna 2 e 3.





Union-Based SQLi - Exemplo

Sabendo que é a coluna 2 e 3 a ser mostrada pela aplicação, podemos agora adaptar a nossa injeção SQL para mostrar nestas colunas o nome do usuário com que estamos a acessar ao banco de dados e o nome do banco de dados. Neste caso o nome do usuário é acuart@localhost e o nome do banco de dados é acuart.