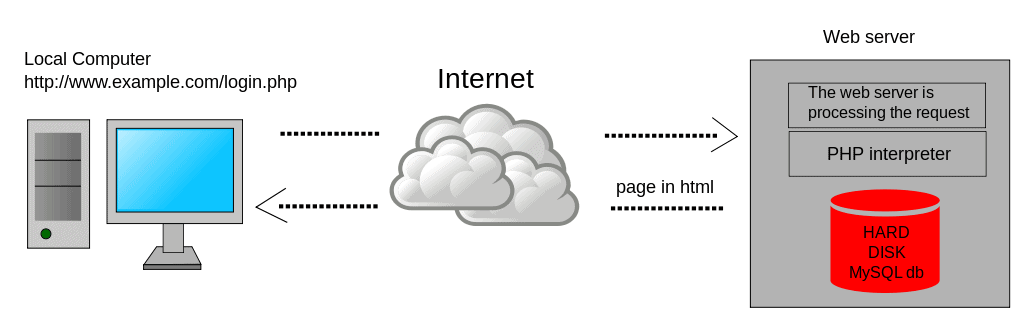
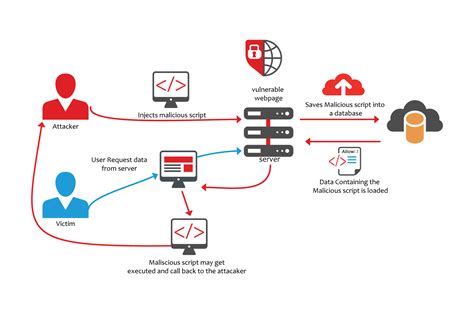
Home SIEM Lab

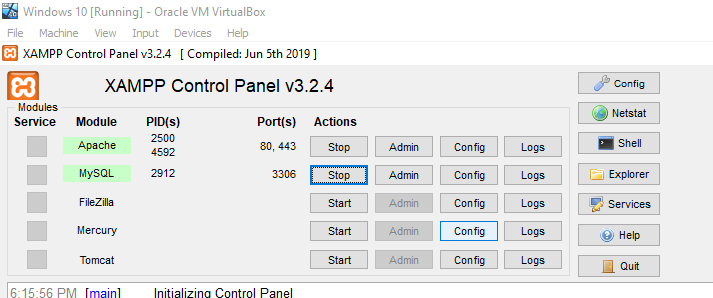
In this lab I will configure a web Server application using XAMPP hosted on my local machine, Splunk will be configured to collect data from log files and trigger alerts if SQL injection(SQLI) or cross site scripting(XSS) are performed.

Apache will be used to host the Server and create an interface for the frontend, I will create a data base on the backend using MySQL that will hold information that is input onto the website. PHP will be the middle man interacting with both the backend and frontend taking input from the HTML pages and storing them in the SQL database. Splunk will be configured watch and collect data from the PHP log files and trigger an alert if it detects SQLI or XSS attempts.





XAMPP Services and Ports



MySQL server running on Apache local host(127.0.0.1) with php configurations

A screenshot of a computer

Description automatically generated

php config files

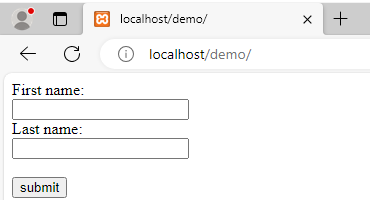
A group of numbers on a white background

Description automatically generated

php config to create input for database variables

A screenshot of a computer program

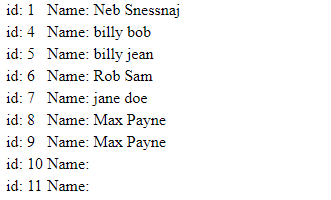
Description automatically generated



php config to push variables to MySql and display variables on web browser

A screenshot of a computer program

Description automatically generated



Selecting host view a data summary from splunk

A screenshot of a computer

Description automatically generated

Splunk detecting input from Web Application

A screenshot of a computer

Description automatically generated

Performing SQLI and XSS on the web application to modify the backend



A screenshot of a computer

Description automatically generated

A red square with black text

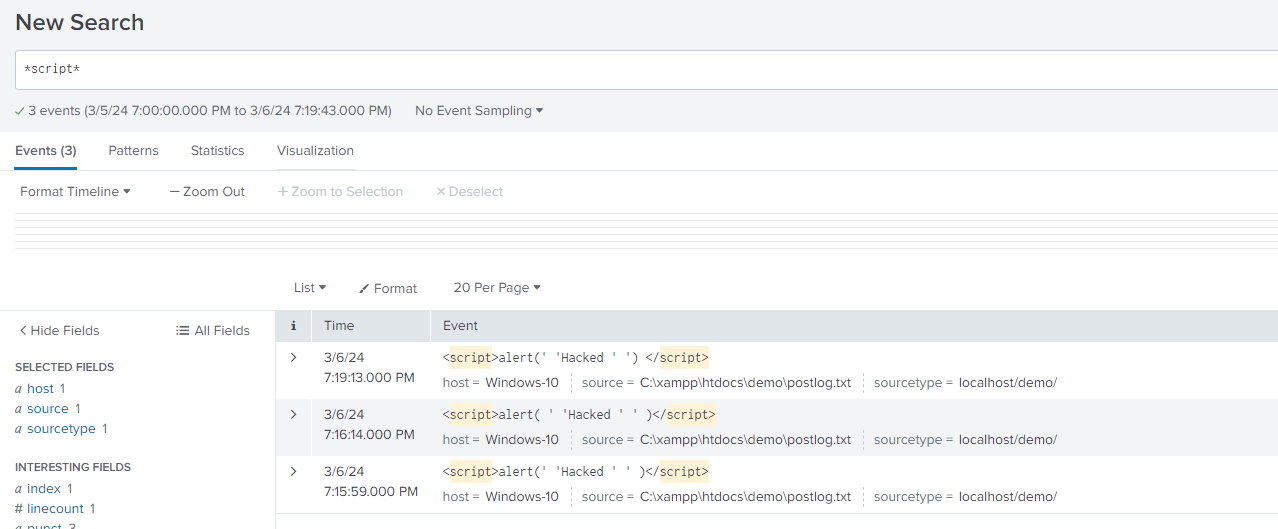
Description automatically generated

A screenshot of a computer

Description automatically generated



Creating Alerts for Splunk to detect SQLI and XSS



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Realtime detection of triggered events

