Report Findings

Based on the anomaly detection model and visualizations:

1. **Suspicious Sessions Detected**
    - The Isolation Forest model successfully classified a portion of the web traffic as **Suspicious**.
    - These sessions typically exhibit **unusual traffic patterns** compared to normal connections.
2. **High Bytes In with Low Bytes Out**
    - Many suspicious connections have **very high incoming bytes** but relatively low outgoing bytes.
    - This could indicate potential **data infiltration attempts** or **probing attacks**.
3. **Country Code Patterns**
    - Certain country codes have a **higher frequency of suspicious interactions**, suggesting **targeted or bot-driven activity** from specific regions.
4. **Port Usage**
    - While most traffic is on **standard HTTPS port 443**, suspicious sessions sometimes occur on **non-standard ports**, potentially signaling **unauthorized access attempts**.
5. **Visual Trends**
    - The scatter plot of Bytes In vs Bytes Out shows clear separation between **normal** and **suspicious** sessions, validating the model's effectiveness.

Conclusion

The analysis demonstrates how machine learning (Isolation Forest) can identify anomalous patterns in real-time web traffic. By integrating such models into monitoring systems, organizations can enhance their **intrusion detection capabilities**, proactively identifying and mitigating cyber threats before they cause harm.