Name- Russel B Rex
Reg.no- EA2352001010458

WEEK-15 LAQ

Security Tools in E-commerce.

E-commerce security is paramount for businesses to protect customer data and build trust. Here are some key security tools and strategies employed:

1. Secure Sockets Layer (SSL) / Transport Layer Security (TLS):

- **What it does:** Encrypts communication between the website and the user's browser, safeguarding sensitive data like payment information and personal details during transmission.
- **How it works:** An SSL certificate issued by a trusted Certificate Authority (CA) is installed on the web server. This establishes a secure connection, indicated by the "https://" in the URL and the padlock icon in the browser.

2. Firewalls:

- **What they do:** Act as a barrier between the e-commerce website and external networks, blocking unauthorized access and malicious traffic.
- **Types:** Hardware firewalls are physical devices, while software firewalls are installed on individual computers or servers.

3. Intrusion Detection and Prevention Systems (IDS/IPS):

- **What they do:** Monitor network traffic for suspicious activity and alert administrators or automatically block potential threats.
- **How it works:** IDS detects anomalies and alerts, while IPS actively blocks malicious traffic based on predefined rules.

4. Web Application Firewalls (WAFs):

- **What they do:** Protect against common web vulnerabilities like SQL injection, cross-site scripting (XSS), and other attacks that target web applications.
- **How it works:** WAFs analyse incoming web requests, filtering malicious traffic and blocking potential exploits.

5. Secure Data Storage:

- **What it does:** Protects sensitive data stored on servers and databases by implementing various security measures.
- **Key methods:**

    - **Data encryption:** Encrypting data at rest using algorithms and keys, making it unreadable without proper decryption.
    - **Access control:** Limiting user permissions based on roles and responsibilities, granting only necessary access to data.
    - **Data masking:** Hiding sensitive data while still allowing for use in applications, protecting privacy while maintaining functionality.

6. Secure Payment Gateways:

- **What they do:** Handle payment processing securely, encrypting sensitive payment information and ensuring compliance with industry standards like PCI DSS.
- **How it works:** Integrate with trusted payment gateways like Stripe, PayPal, or Braintree, which handle the complexities of payment security.

7. Two-Factor Authentication (2FA):

- **What it does:** Adds an extra layer of security by requiring users to provide two different authentication factors (e.g., password and a code sent to their phone).
- **How it works:** Makes it harder for unauthorized individuals to access accounts, even if they obtain a password.

8. Vulnerability Scanning:

- **What it does:** Regularly scans the website and network for potential security vulnerabilities, identifying weaknesses that could be exploited.
- **How it works:** Uses automated tools to check for known vulnerabilities and misconfigurations, allowing for timely patching and remediation.

9. Security Awareness Training:

- **What it does:** Educates employees about cybersecurity threats, best practices, and procedures to prevent data breaches.
- **How it works:** Helps employees recognize phishing attempts, understand password security, and report suspicious activity.

10. Incident Response Plan:

- **What it does:** Outlines a structured plan to respond to security incidents and data breaches, minimizing damage and ensuring swift recovery.
- **How it works:** Defines roles, responsibilities, communication channels, and steps to contain the incident, investigate the root cause, and restore affected systems.

11. Data Loss Prevention (DLP):

- **What it does:** Prevents sensitive data from leaving the company's network, protecting it from unauthorized access or theft.
- **How it works:** Uses various techniques like data encryption, access control, and monitoring of data transfers.

12. Continuous Monitoring:

- **What it does:** Actively monitors the website, network, and systems for suspicious activity and potential security breaches.
- **How it works:** Uses security information and event management (SIEM) tools to collect, analyse, and correlate security data, providing real-time visibility into potential threats.

Remember: E-commerce security is an ongoing process that requires continuous vigilance and adaptation to evolving threats. Regular security audits, updates, and employee training are essential to protect customer data and maintain trust in your online business.