Report on Flipkart web app security

Name: Prasanna Tangade
Roll No: C_71 Subject: Application Security
Course code : CCT310-3
Department: CSE(Cyber Security) Section: C

Introduction:

In today's world, online shopping is becoming increasingly popular, and Flipkart is one of the most popular e-commerce platforms in India. Flipkart is a web application that serves millions of users every day. It is essential to ensure that the web application is secure and that customers' data is protected from cyber threats. In this essay, we will discuss Flipkart's comprehensive security planning, analysis, and review by referring to the OWASP Top 10.

OWASP Top 10:

OWASP Top 10 is a list of the most critical web application security risks. These risks are ranked according to their severity and potential impact on web applications. The list is updated every three years to ensure that it reflects the latest security threats.

Comprehensive Security Planning:

A comprehensive security plan is necessary for Flipkart to ensure that the web application is secure. The plan should include various security measures, such as access control, authentication, encryption, and network security. The following are some of the security measures that Flipkart can implement:

1. Access Control: Access control is an essential aspect of web application security. Flipkart can implement access control by

ensuring that only authorised users can access the web application. Access control can be achieved by implementing password policies, multi-factor authentication, and role-based access control.
2. Authentication: Authentication is the process of verifying the identity of a user. Flipkart can implement authentication by using secure authentication mechanisms such as OAuth, OpenID Connect, and SAML.
3. Encryption: Encryption is the process of converting data into a secure format that can only be read by authorized users. Flipkart can implement encryption by using SSL/TLS protocols to secure data in transit and using encryption algorithms to secure data at rest.
4. Network Security: Network security is essential to protect Flipkart's web application from cyber threats. Flipkart can implement network security by using firewalls, intrusion detection and prevention systems, and VPNs.

Analysis:

Flipkart can conduct a comprehensive analysis of its web application to identify vulnerabilities and security gaps. The analysis should include both manual and automated testing to identify security weaknesses. The following are some of the testing methods that Flipkart can use:

1. Vulnerability Scanning: Vulnerability scanning is the process of identifying vulnerabilities in a web application. Flipkart can use automated vulnerability scanning tools to identify vulnerabilities in the web application.
2. Penetration Testing: Penetration testing is the process of simulating a cyber-attack to identify vulnerabilities in a web

application. Flipkart can use ethical hacking techniques to identify weaknesses in the web application.
3. Code Review: Code review is the process of reviewing the code for security vulnerabilities. Flipkart can conduct code reviews to identify security flaws in the web application's code.

Review:

After conducting a comprehensive analysis, Flipkart can review the findings to identify vulnerabilities and security gaps. The review should prioritize the findings based on their severity and potential impact on the web application. The following are some of the vulnerabilities that Flipkart may find during the review:

1. Injection Attacks: Injection attacks occur when an attacker injects malicious code into a web application. Flipkart can prevent injection attacks by validating user input and using parameterized queries.
2. Cross-Site Scripting (XSS): Cross-site scripting is a type of attack that occurs when an attacker injects malicious code into a web page. Flipkart can prevent XSS attacks by sanitizing user input and using Content Security Policy (CSP).
3. Broken Authentication and Session Management: Broken authentication and session management occur when an attacker hijacks a user's session or gains unauthorized access to the web application. Flipkart can prevent these attacks by implementing secure authentication and session management mechanisms.

In addition to referring to the OWASP Top 10, Flipkart can also benefit from referring to the reports published by PurpleSec, a leading cybersecurity company. PurpleSec publishes reports on the latest cyber threats and vulnerabilities, and Flipkart can use these reports to enhance its security planning, analysis, and review.

PurpleSec's reports cover a wide range of topics, including threat intelligence, vulnerability management, incident response, and security best practices. By analysing these reports, Flipkart can gain insights into the latest security threats and vulnerabilities that may impact its web application.

For example, PurpleSec's report on the top cyber threats in 2021 highlights the growing threat of ransomware and supply chain attacks. Flipkart can use this information to implement additional security measures to protect against these types of attacks.

PurpleSec's reports also provide actionable recommendations for mitigating security risks. For example, the report on vulnerability management recommends implementing a vulnerability management program that includes regular vulnerability scans, penetration testing, and patch management.

Flipkart can use these recommendations to enhance its security planning, analysis, and review processes. By implementing these recommendations, Flipkart can reduce its risk of cyber attacks and protect its customers' data.

In conclusion, referring to the reports published by PurpleSec can be a valuable resource for Flipkart's comprehensive security planning, analysis, and review processes. By leveraging the latest cybersecurity insights and recommendations, Flipkart can enhance its web application's security and protect against the latest threats and vulnerabilities.