Threat Event	Threat Source	Vulnerabilities	Impact	Asset	Overall Likelihood	Level of Impact	Security Controls
Customers' browser infected by Trojan and this leads to alteration of transaction data	Hacker	1. Poor security awareness 2. Weak malware protection	Unauthorized transaction via web application	Integrity of account data	Likely	Severe	1. Regularly inform customers about security best practices. 2. Strengthen authentication of transaction in web application.
Keylogger installed on computer and this leads to sniffing customer credentials. Which leads to unauthorized access to customer account via web application.	Cyber criminal	Insufficient detection of spyware	Unauthorized transaction via web application	Integrity of account data	Likely	Severe	Strengthen authentication of transaction in web application.
Spear-phishing attack on customers leads to sniffing customer credentials. Which leads to unauthorized access to customer account via web application.	Cyber criminal	Poor security awareness	Unauthorized transaction via web application	Integrity of account data	Likely	Severe	1. Regularly inform customers about security best practices. 2. Strengthen authentication of transaction in web application.
Keylogger installed on customer's computer and this leads to sniffing customer credentials	Cyber criminal	Insufficient detection of spyware	Unauthorized access to customer account via web application	User authenticity	Certain	Severe	
Spear-phishing attack on customers leads to sniffing customer credentials	Cyber criminal	Poor security awareness	Unauthorized access to customer account via web application	User authenticity	Certain	Severe	Regularly inform customers about security best practices.
Keylogger installed on customer's computer leads to sniffing customer credentials	Cyber criminal	Insufficient detection of spyware	Unauthorized access to customer account via web application	Confidentiality of customer data	Certain	Severe	
Spear-phishing attack on customers leads to sniffing customer credentials	Cyber criminal	Poor security awareness	Unauthorized access to customer account via web application	Confidentiality of customer data	Certain	Severe	Regularly inform customers about security best practices.
Fake banking app offered on application store and this leads to sniffing customer credentials	Cyber criminal	Lack of mechanisms for authentication of app	Unauthorized access to customer account via fake app	User authenticity	Likely	Critical	Conduct regular searches for fake apps.
Fake banking app offered on application store and this leads to sniffing customer credentials	Cyber criminal	Lack of mechanisms for authentication of app	Unauthorized access to customer account via fake app	Confidentiality of customer data	Likely	Severe	Conduct regular searches for fake apps.
Fake banking app offered on application store leads to sniffing customer credentials. Which leads to unauthorized access to customer account via fake app.	Cyber criminal	Lack of mechanisms for authentication of app	Unauthorized transaction via Poste App	Integrity of account data	Unlikely	Minor	Conduct regular searches for fake apps.
Fake banking app offered on application store leads to alternation of transaction data	Cyber criminal	Lack of mechanisms for authentication of app	Unauthorized transaction via Poste App	Integrity of account data	Unlikely	Minor	Conduct regular searches for fake apps.
Smartphone infected by malware and this leads to alteration of transaction data	Hacker	Weak malware protection	Unauthorized transaction via Poste App	Integrity of account data	Unlikely	Minor	Regularly inform customers about security best practices.
Denial-of-service attack	Hacker	1. Use of web application 2. Insufficient resilience	Online banking service goes down	Availability of service	Certain	Minor	1. Monitor network traffic. 2. Increase bandwidth.
Web-application goes down	System failure	Immature technology	Online banking service goes down	Availability of service	Certain	Minor	Strengthen verification and validation procedures.