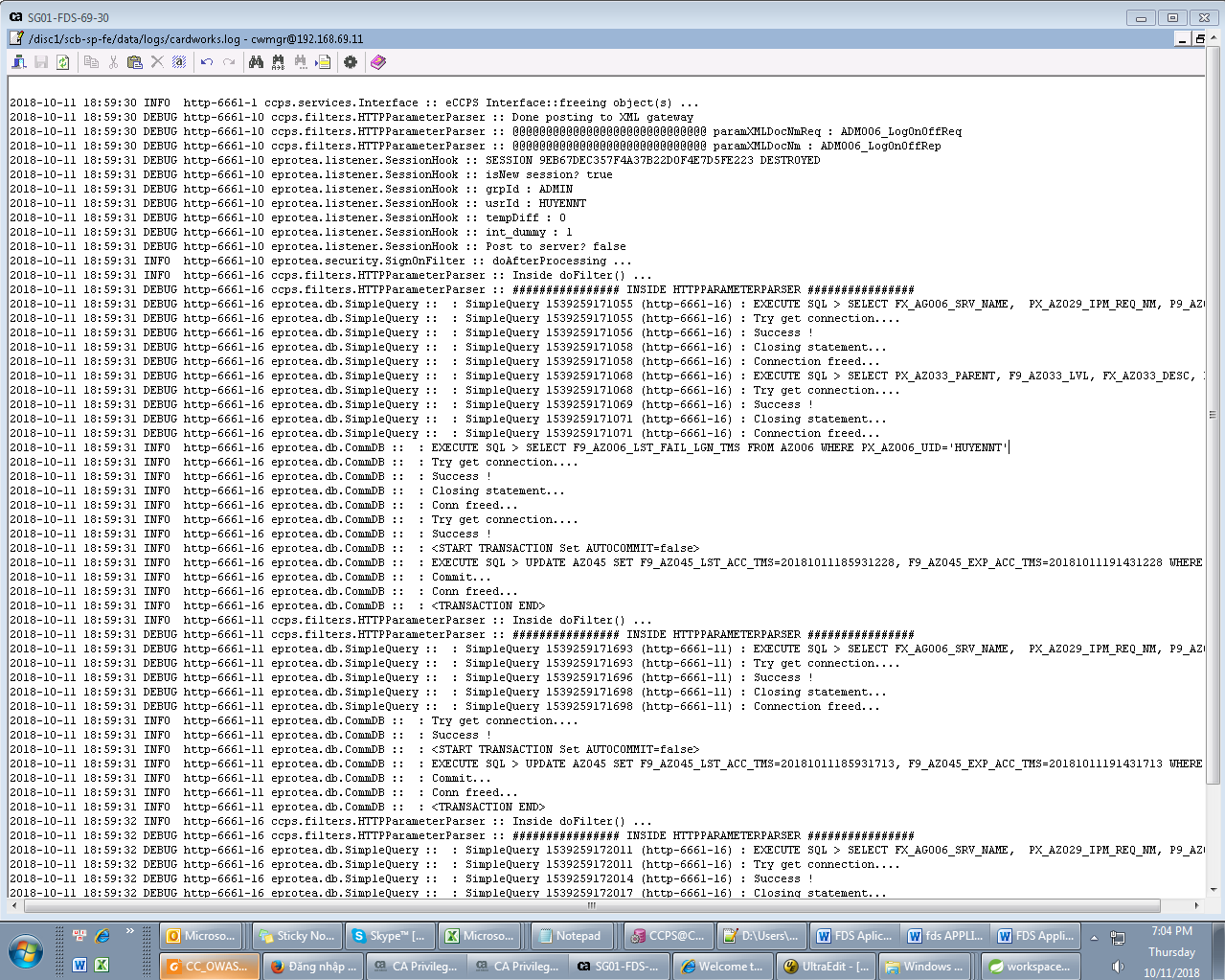
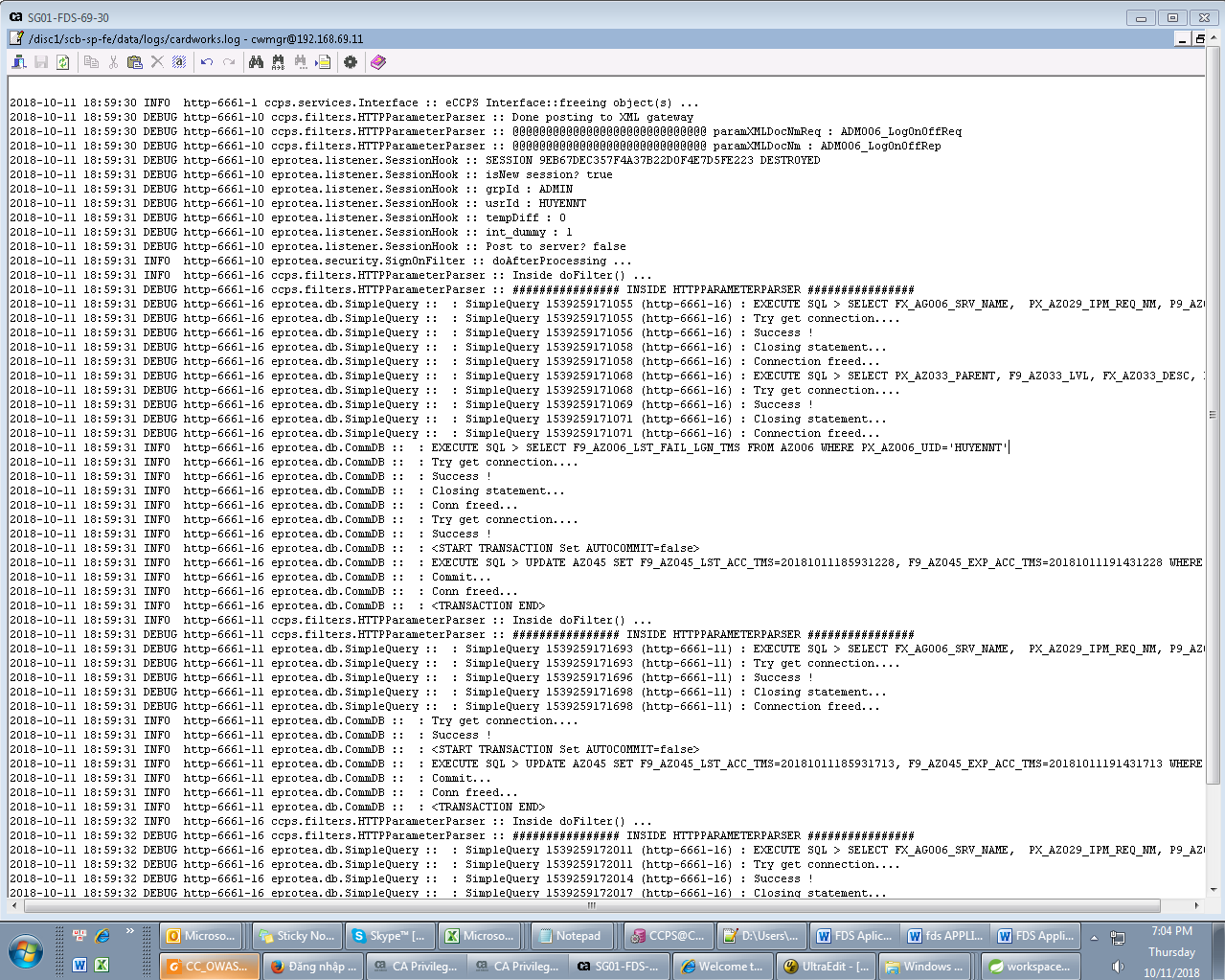
Cardworks Application 2019

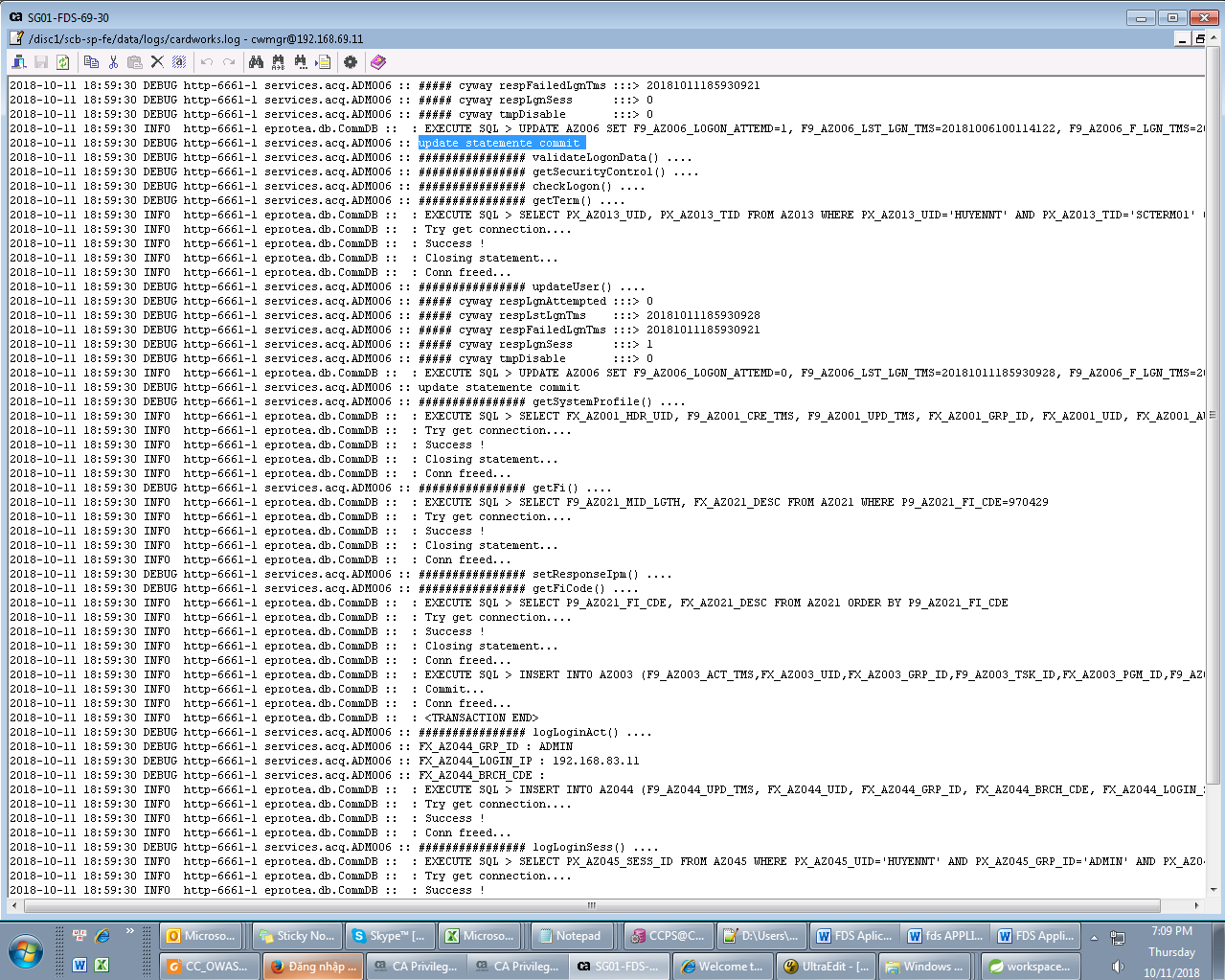
A10-Insufficient Logging & Monitoring Controlshttps://cardworks.scb.com.vn/scb/prod/safe2pay-hostadmin/index.html  
1-Ensure all login, access control failures, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts, and held for sufficient time to allow delayed forensic analysis.



2-Ensure that logs are generated in a format that can be easily consumed by a centralized logmanagement solutions.



3-Ensure high-value transactions have an audit trail with integrity controls to prevent tampering ordeletion, such as append-only database tables or similar.



4-Establish effective monitoring and alerting such that suspicious activities are detected and responded to in a timely fashion.

(Mr.Tho will Snap shot of the Antivirus Alert)

5-Establish or adopt an incident response and recovery plan, such as NIST 800-61 rev 2 or later.XYZ Company have the Incident response & recovery plan in place. Please find the below snap shot.

6-logs are move from local server to central repository.

7-Provide the logs of all testing requests and payload that we had performed on applications this will show logging is enabled for application.

