REQUIREMENT ENGINEERING AND THREAT MODELLING PROJECT SUBMITTED BY BRIGHT CHUKWUEBUKA JIWUEZE. IN PARTIAL FUFILMENT OF THE AWARD OF HDBW M.Sc. IN CYBER SECURITY.

In Subaac company, we are majorly into real estate investment. At some point, we realized that in other to streamline our accounting information and give our customers the best service, we need a web & mobile app that would help us track expenses, payments & create professional invoices & estimates the customers could make payments through the app and generate invoice easily from the app. In addition, for better streamlined financial operation, the company through the account officer also uses this app internally for all financial engagements. The admin oversees permissions in the app.

This application is to be developed internally by our web developers and the name of the application is **crater**, which will perform all the tasks mentioned above. Users have access to perform various services through APIs. They first get a token from an authentication server through an API after submitting the required credentials. That token would be requested from users to grant them access to other protected endpoints.

Stakeholder Analysis

Role	**Name**	**Availability**	**Know-How**	**Problems and Needs**	**Business Relevance**	**Security Relevance**
Business Manager	Alan Tur	Frequently	In charge of the overall functionality of the business.	Customer satisfaction by providing the best service.	Decision maker	Fulfil compliance
Security manager	Bright Jiwueze	Frequently	Knows information security requirement.	Avoid security breaches, that could disrupt the business and affect company's reputation.	No business relevance	Full interest in security
Data protection officer	Chris john	Selectively available	Knows data protection requirement.	Protect personal and financial	No business relevance	Compliance relevance

				information using GDPR and PCI DSS.		
Admin	Alice Benson	Frequently	Knows permissions and privileges within the organization's IT domain.	Users should be granted permissions base on specific needs.	No business relevance	Full interest in security
Customer Representative	Fred Bown	Selectively available	Interested in the best service provider.	Customers retention.	Represent the customer segment	Less security relevance
Account officer	Mike Isaac	Frequently	Knows financial transactions of the business.	Safe keeping of the organization's financial records.	monitor payments and issuing of invoice, also granting refunds when necessary	Medium security interest
Web developer	Bill Clinton	Selectively available	Orchestrates the business requirements into a functional application.	Produce a functional app to suite business requirement.	No business relevance	Security by design

RISK PROFILE

We define the protection requirement guidelines Subaac Real Estate Service uses on their IT applications.

Protection level	**General description**	**DEFINTION**
Normal	The impact of any loss or damage has no effect to the business process	The overall costs are lower than 10 % of the annual turnover. There is no reputational damage
High	The impact of any loss or damage may be considerable	The overall costs are between 10% and 40% of the annual turnover

		OR there is a bit loss of reputation.
Very High	The impact of any loss or damage may be of catastrophic proportions which could threaten the very survival or the organization.	The overall costs are higher than 40 % of the annual turnover and there is a noticeable loss of reputation.

CRATER DATA CLASSIFICATION

DATA	DETAIL	PROTECTION LEVEL	SECURITY OBJECTIVE	RATIONAL
Unprivileged Users Authentication token	The token that a user receives in that grants access to other secured APIs/endpoints	High	C, I, A	It affects a particular user. Might cause damage and changes to the user's data. A bit effect on the company's reputation
User credentials	name, email, phone number, ….	Normal	C	An attacker even with the credentials won't still have access into the application without the authentication token
Customers Payment details	Card number, CVE, Expiry dates	Very High	C, I, A	This can cause a big damage to company's reputation and those information could be deleted after

				theft that the records won't be available in the server anymore
Invoices	Customer's proof of successful business transaction	High	C, I, A	The invoice can leak customers information and may affect account audit if been deleted by the hacker. Pose a bit threat to the reputation of the business
Company's account information	The record of companies Income and expenses	Very High	C, I, A	This poses a great damage to the reputation of the company, e.g. having to find such a company's account information in the dark web
Admin login Credentials	Credentials that grant access to the admin page	Very High	C, I, A	An attacker having access to any admin login credentials can use it to perform any attack of his choice.
Unprivileged User session cookies	user information	High	C, I, A	An attacker can intercept user's cookies,

	during website access			use it and perform any function on behalf of the user

DAMAGE SCENARIO

Damage Scenario	**Potential Attackers**	**Criticality**	**Rational**
An attacker can steal customers authentication token, retrieve customers payment information and use it to make a purchase.	Motivated/paid hacker	High	Affects a particular user alone
An attacker can trace the algorithm for generating the authentication, use it to brute force the APIs	Inside threat Motivated/paid hacker	High	Can only perform unprivileged tasks just like other customers that uses token for authentication
An attacker can get the account officer through phishing attack.	Motivated/paid hacker	Very High	A threat to the account information of the company
An attacker can leverage a plugin that poses zero-day threat, create new admin user through it and get access to the admin page of the web app	Motivated/paid hacker	Very High	The hacker has taken over the system, can create a reverse shell, then perform other tasks.

SECURITY USER STORIES

As a customer of Subaac, I would like my personal information and credit/debit card details to be protected from access by hackers, so the money in my personal bank account will not be exploited using those details.

Acceptance Criteria

- Ensure that the transfer of data from the customer's browser to the web server is encrypted with TLS 1.3.
- Ensure that only authenticated and authorized users have access to customer data via the crater.
- Ensure that my authentication token is been sent to me through an encrypted channel.

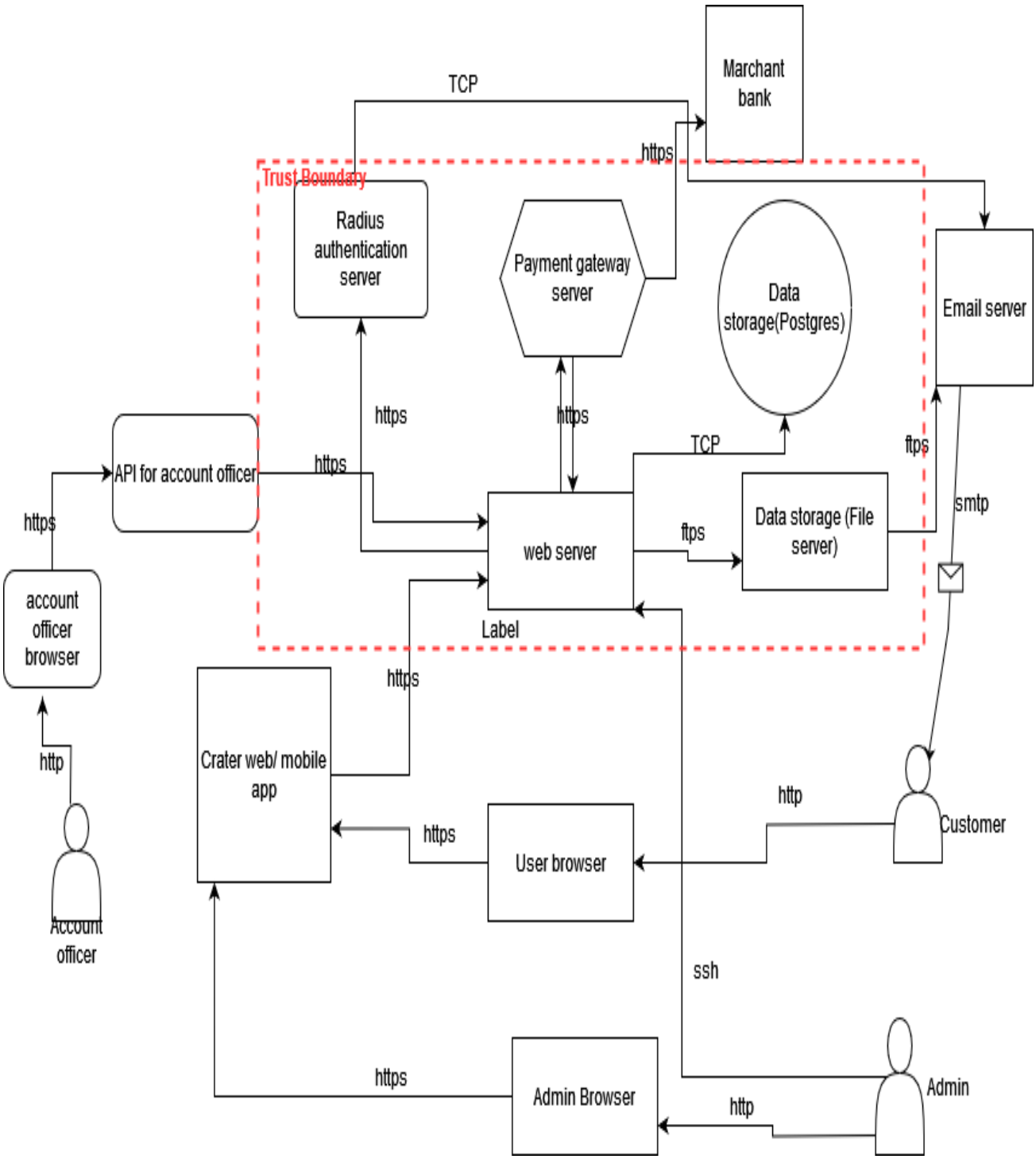
EVIL STORY

As a hacker, I would like to access the personal data and credit/debit card details of all customers of Subaac Real Estate Investment, so I could use their card details to steal their money from their bank account and damage the reputation of Subaac real estate services, also have access to the account information of the said company and sell my findings in the dark web.

Acceptance Criteria

- Data of interest is: Personal data (e.g. age, first name, last name, gender), Credit/debit card information, and customers authentication token.
- Company’s financial account information.

THREAT MODEL



THREAT DOCUMENTATION USING STRIDE

STRIDE	MODEL	THREAT	POSSIBLE DEFENSE
Spoofing	Customers, Admin, and Account officer	Authentication token theft, using phishing to convince users to perform actions	Security awareness, SPF, DKIM, Multi factor Authentication
Tampering	Database, file storage, transaction process	Attackers can hijack admin, account officers' session, or take advantage of a vulnerable plugin to have admin access through XSS and then manipulate the data.	Session cookies encryption, Security research for zero-day. Use updated plugins
Repudiation	Trust boundary Area	The system will not be able to trace who performed a particular activity	Implementing log capture and users' session cookies, user identification using various authentication methods
Information Disclosure	Database, file storage and payment gateway server.	Data breach. Attacker can be disclosed to customers payment details as well as company's financial records.	Security awareness, least privilege, encryption e.tc.
Denial of service	Webserver, Database, file	Services not available	IP blocking, Rate limiting, Captcha.

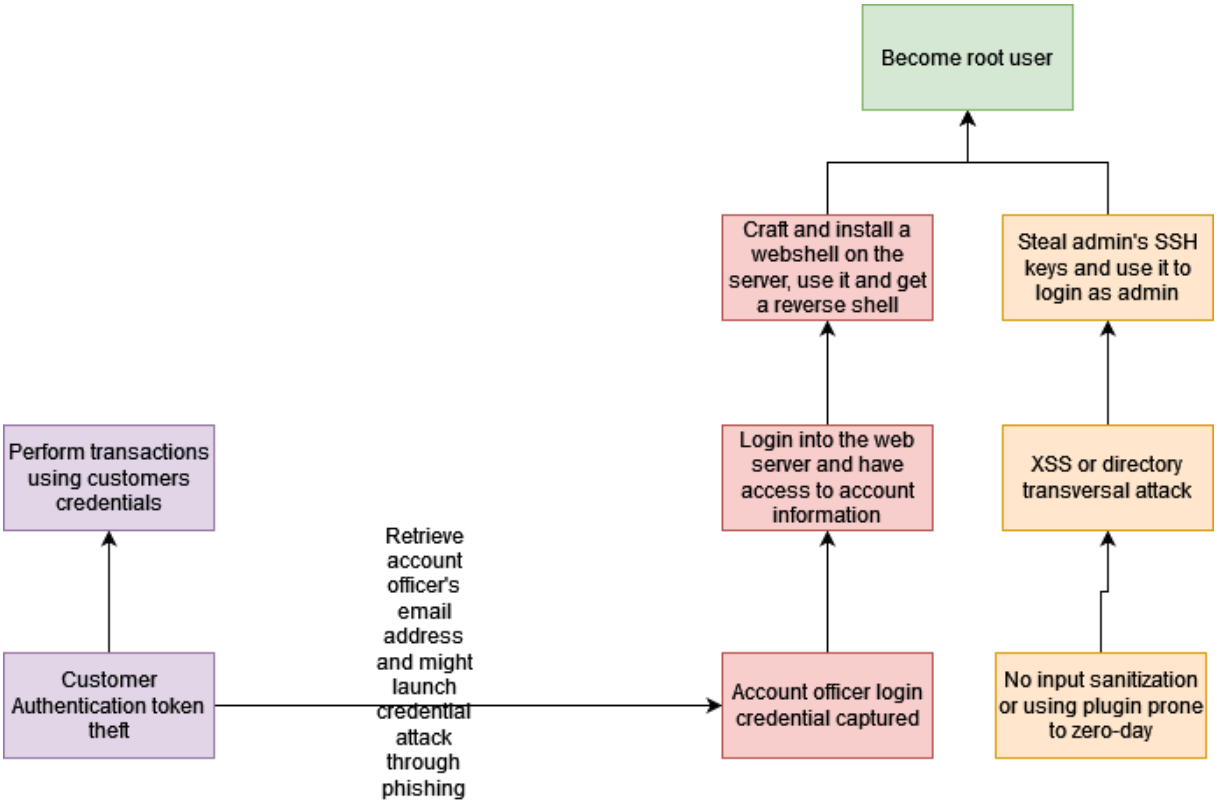
	storage and payment gateway server.		
Elevation privilege	Privilege and Unprivileged users	Reverse shell, root actions	Principle of least privileges, Zero trust

RISK EVALUATION USING OWASP RISK RATING https://owasp-risk-rating.com/

RISK	LIKELIHOOD	SEVERITY	IMPACT
Authentication token theft, using phishing to convince users to perform actions	Medium	High	High
Attackers can hijack admin, account officers' session, or take advantage of a vulnerable plugin to have admin access through XSS and then manipulate the data	Medium	High	High
The system will not be able to trace who performed a particular activity	Medium	Medium	Medium
Data breach, Attacker can be disclosed to customers payment details as well as company's financial records.	Medium	High	High

Services not available	Medium	High	High
Reverse shell, root actions	medium	High	High

ATTACK TREE



THREAT DECISION: WHICH THREATS WOULD YOU MITIGATE? WHAT SECURITY MEASURES WOULD YOU IMPLEMENT?

Threats listed in this document regarding to the **crater** web and mobile application poses a great risk to Subaac real estate investment and all should be mitigated in other to be in compliance with the PCI DSS standard https://www.pcisecuritystandards.org/ and the GDPR https://gdpr.eu/.

Based on the risks detected, risk avoidance, transfer, and accepting won't play a better role in this scenario.

SECURITY MESURES TO IMPLEMENT

- Send users authentication tokens through encrypted channels.
- Security Training and Awareness using PCI DSS and GDPR guidelines.
- Principle of least privileges
- Updated components and plugins
- Reduction of attack surfaces
- Implementing syslog and webhooks
- Input sanitization, directory traversal attacks can grant access to the root directory up to /admin/.ssh/ folder and might leak ssh keys.
- Multi factor authentication for the account officer's API

REFERENCES

- https://crater.financial/
- https://gdpr.eu/
- https://github.com/crater-invoice/crater
- https://owasp-risk-rating.com/
- https://www.pcisecuritystandards.org/